

Patent Application Laid-Open No. H 10-135945

Laid-Open Date: May 22, 1998

Patent Application No. H 8-291452

Application date: November 1, 1996

No Examination Requested

Applicant: K.K. Toshiba

Inventors: June Inoue et al

Title of the Invention:

Mobile Computer, Packet Processing Apparatus and Communication Controlling  
Method

Corresponding United States Patent Number 6.167,513

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-135945

(43)公開日 平成10年(1998) 5月22日

(51)Int.Cl. <sup>4</sup>	識別記号	F I
H 0 4 L 9/32	---	H 0 4 L 9/00 6 7 1
G 0 6 F 13/00	3 5 5	G 0 6 F 13/00 3 5 5
	15/00	15/00 3 3 0 A
H 0 4 L 12/56	3 3 0	H 0 4 L 11/20 1 0 2 Z

審査請求 未請求 請求項の数23 O L (全 36 頁)

(21)出願番号 特願平8-291452

(22)出願日 平成8年(1996)11月1日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 井上 淳

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72)発明者 石山 政浩

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72)発明者 福本 淳

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(74)代理人 弁理士 鈴江 武彦 (外6名)

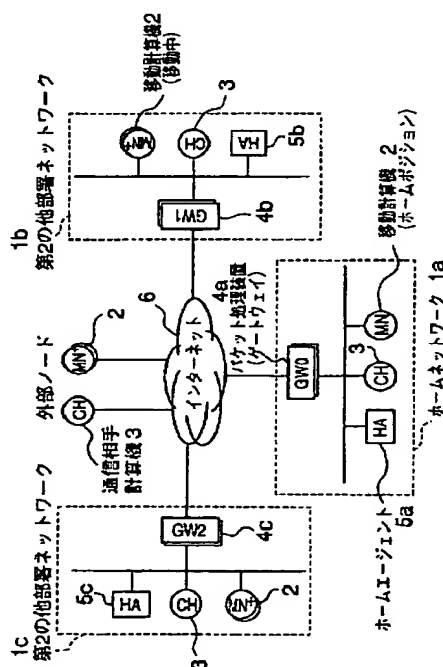
最終頁に続く

(54)【発明の名称】 移動計算機装置、パケット処理装置及び通信制御方法

(57)【要約】

【課題】 自装置の現在位置に応じて移動情報の登録、通信相手へのパケット転送を正しく行えるようにした移動計算機装置を提供すること。

【解決手段】 ホームネット内の計算機がネット外へ向けて送信するパケットを暗号化認証処理する機能を持つパケット処理装置が設置されたネットワークを含む複数のネットワークが相互接続された通信システム内を移動通信可能な移動計算機装置であって、自装置が、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する管理装置の設置されたホームネット内に位置するか否かを認識する手段と、自装置及び自装置が通信相手とする計算機の少なくとも一方につきその送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識する手段と、これら認識結果に基づき、送信すべきパケットの暗号化認証処理を含む所定の通信処理を行う手段とを具備する。



## 【特許請求の範囲】

【請求項1】ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置が設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内を移動して通信を行うことが可能な移動計算機装置であって、

自装置が、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークの内部に位置するか外に位置するかを認識する第1の認識手段と、自装置及び自装置が通信相手とする計算機の少なくとも一方につき、その送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識する第2の認識手段と、

これら第1及び第2の認識手段の認識結果に基づき、送信すべきパケットの暗号化認証処理を含む所定の通信処理を行う手段とを具備することを特徴とする移動計算機装置。

【請求項2】前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識された場合、該移動計算機管理装置へ向けて、所定の暗号化認証処理を施した、自装置の現在位置情報を含む登録メッセージを送信し、

これに対し経路途中のパケット処理装置から通過拒否応答が返信された場合、該パケット処理装置の認証用鍵情報を検索し、この認証用鍵を使った認証コードを登録メッセージに付加して再送信することを特徴とする請求項1に記載の移動計算機装置。

【請求項3】前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識された場合、該ネットワークの内部の前記移動計算機管理装置へ向けて、現在位置情報を含む登録メッセージを、暗号化認証処理せずに送信することを特徴とする請求項1に記載の移動計算機装置。

【請求項4】前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識された場合、自装置が通信相手とする計算機に向けて、暗号化認証処理せずにパケットを送信することを特徴とする請求項1に記載の移動計算機装置。

【請求項5】前記第2の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、そのパケット処理装置が一致すると認識された場合、

自装置が通信相手とする計算機に向けて、暗号化認証処

理せずにパケットを送信することを特徴とする請求項1に記載の移動計算機装置。

【請求項6】前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とする他のパケット処理装置が存在すると認識され、さらに、既に該パケット処理装置が自装置の送信するパケットを認証処理なしに外部へ通過させるものであることが判明している場合、

自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データを付加されたパケットを送信することを特徴とする請求項1に記載の移動計算機装置。

【請求項7】前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とする他のパケット処理装置が存在すると認識され、さらに、既に該パケット処理装置が自装置の送信するパケットを認証処理なしに外部へ通過させないものであることが判明している場合、

自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データおよび経路間認証データの付加されたパケットを送信することを特徴とする請求項1に記載の移動計算機装置。

【請求項8】前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識された場合、

自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データの付加されたパケットを送信することを特徴とする請求項1に記載の移動計算機装置。

【請求項9】前記第2の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識され場合、

自装置が通信相手とする計算機に向けて、暗号化認証処理せずにパケットを送信することを特徴とする請求項1に記載の移動計算機装置。

【請求項10】前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置

されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識された場合、

自装置が通信相手とする計算機との間で、暗号通信は行わず、かつ、自装置が移動先で獲得したアドレスを使用して通信相手となる計算機と直接通信することを特徴とする請求項1に記載の移動計算機装置。

【請求項11】前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在せず、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識された場合、

自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークに対して所定の通信内容が暗号化されたパケットを送信し、該ネットワーク内のパケット転送装置によりアドレスを変換して自装置が通信相手とする計算機に転送してもらうとともに、

自装置が通信相手とする計算機から送信されるパケットは、該パケット転送装置によりアドレス変換した後に、移動計算機管理装置で経路制御し、所定の通信内容を暗号化して自装置に転送してもらうことを特徴とする請求項1に記載の移動計算機装置。

【請求項12】ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内に設置され、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置であって、

転送すべきパケットの送信元となる計算機及び宛先となる計算機の少なくとも一方について、その計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機か否かを認識する第1の認識手段と、

前記計算機の少なくとも一方について、その計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識する第2の認識手段と、これら第1及び第2の認識手段の認識結果に基づき、前記計算機間で通信されるパケットの暗号化認証処理を含む所定の通信処理を行う手段とを具備することを特徴とするパケット処理装置。

【請求項13】前記第2の認識手段により、自装置が該

移動計算機が送信するパケットを暗号化認証処理対象とすることが認識された場合、

前記移動計算機から、自装置宛の経路認証データの付加されていないパケットを受信したならば、通過拒否メッセージを前記移動計算機に返信し、

前記移動計算機から、自装置宛の経路間認証データの付加されたパケットを受信したならば、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段ノードに対する経路間認証データに換えて転送し、

前記計算機宛の応答メッセージを受信したならば、自装置宛の経路間認証データを検査し、該経路間認証データの正当性が確認されたならば、該経路間認証データを除いて前記移動計算機に転送し、

自装置が前記移動計算機管理装置の設置されたネットワークに位置する場合、

前記移動計算機管理装置からの応答メッセージを受信したならば、所定の通信内容を暗号化しかつ末端認証データ及び次段ノードに対する経路間認証データを付加して該応答メッセージを前記移動計算機に宛てて転送することを特徴とする請求項12に記載のパケット処理装置。

【請求項14】前記第1の認識手段により、いずれの計算機も、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機ではないと認識され、かつ、前記第1の認識手段により、いずれの計算機についても、その計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、

暗号化されていないパケットが転送されて来たとき、所定の通信内容を暗号化しかつ末端認証データを付加して転送し、所定の通信内容が暗号化されかつ末端認証データを付加されたパケットが転送されて来たとき、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号してパケットを転送することを特徴とする請求項12に記載のパケット処理装置。

【請求項15】前記第1の認識手段により、少なくとも一方の計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であると認識され、前記第2の認識手段により、該一方の計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識され、かつ、前記第1の認識手段及び前記第2の認識手段により、他方の計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機ではなくかつその送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないもの、ではないと認識された場合、

少なくとも転送すべき入力パケットのパケット形式に基づき、前記計算機間で通信されるパケットの暗号化認証

処理を含む所定の通信処理を行うことを特徴とする請求項12に記載のバケット処理装置。

【請求項16】暗号化されていないデータバケットが転送されて来た場合、所定の通信内容を暗号化しかつ末端認証データを付加して転送し、所定の通信内容が暗号化されかつ末端認証データを付加されたバケットが転送されて来た場合、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号してバケットを転送することを特徴とする請求項15に記載のバケット処理装置。

【請求項17】自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であって、自装置が暗号化認証処理対象とするものを送信元とする、所定の通信内容が暗号化されかつ末端認証データを付加されたバケットが転送されて来た場合、次段ノードに対する経路間認証データを付加して転送し、

前記移動計算機を送信元とする、所定の通信内容が暗号化されかつ末端認証データ及び自装置に対する経路間認証データを付加されたバケットが転送されて来た場合、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段ノードに対する経路間認証データに換えて転送することを特徴とする請求項15に記載のバケット処理装置。

【請求項18】自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であって、自装置が暗号化認証処理対象とするものを宛先とする、所定の通信内容が暗号化されかつ末端認証データ及び自装置に対する経路間認証データを付加されたバケットが転送されて来た場合、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送することを特徴とする請求項15に記載のバケット処理装置。

【請求項19】自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機でない計算機であって、自装置が暗号化認証処理対象とするものを宛先とする、所定の通信内容が暗号化されかつ自装置に対する末端認証データ及び経路間認証データを付加されたバケットが転送されて来た場合、該末端認証データ及び該経路間認証データを夫々検査し、該末端認証データ及び該経路間認証データの正当性がいずれも認識されたならば、該末端認証データ及び該経路間認証データを取り除き所定の通信内容を復号して転送することを特徴とする請求項15に記載のバケット処理装置。

【請求項20】自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機を宛先とし、他の計算機を送信元とするバケットであって、該移動計算機管理装置により中継された

とが示されるバケットが転送されてきた場合、該移動計算機を暗号化認証処理対象とするバケット処理装置が存在すると認識されたならば、所定の通信内容を暗号化しかつ該移動計算機に対する末端認証データ及び次段ノードに対する経路間認証データを付加してバケットを転送し、該移動計算機を暗号化認証処理対象とするバケット処理装置が存在しないと認識されたならば、所定の通信内容を暗号化しかつ該移動計算機に対する末端認証データを付加してバケットを転送することを特徴とする請求項15に記載のバケット処理装置。

【請求項21】経路最適化を要求された際に、前記第1及び第2の認識手段による認識結果に基づいて自装置が経路最適化に寄与するものであると認識された場合、前記認識結果に応じた所定の経路最適化処理を行うことを特徴とする請求項12、15、16または17に記載のバケット処理装置。

【請求項22】ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するバケットを暗号化認証処理する手段を有するバケット処理装置が設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内を移動して通信を行うことが可能な移動計算機装置の通信制御方法であって、自装置が、自装置の移動位置情報を管理し自装置宛のバケットを自装置の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークの内部に位置するか外に位置するかを認識するとともに、自装置及び自装置が通信相手とする計算機の少なくとも一方につき、その送信するバケットを暗号化認証処理対象とするバケット処理装置が存在するか否かを認識し、これら認識結果に基づき、送信すべきバケットの暗号化認証処理を含む所定の通信処理を行うことを特徴とする通信制御方法。

【請求項23】ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し該移動計算機宛のバケットを該移動計算機の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内に設置され、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するバケットを暗号化認証処理する手段を有するバケット処理装置の通信制御方法であって、

転送すべきバケットの送信元となる計算機及び宛先となる計算機の少なくとも一方について、その計算機が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機か否かを認識し、

前記計算機の少なくとも一方について、その計算機を送信するバケットを暗号化認証処理対象とするバケット処理装置が存在するか否かを認識し、

これら認識結果に基づき、前記計算機間で通信されるバ

ケットの暗号化認証処理を含む所定の通信処理を行うことを特徴とする通信制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、移動計算機装置、パケット処理装置及び通信制御方法に関する。

【0002】

【従来の技術】計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外、1組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（Internet）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

【0003】また、このようなネットワークの普及に伴い、移動通信（mobile computing）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上のアドレスを管理し、正しく通信内容を到達させるための方式が必要である。

【0004】また、ネットワークが普及し、ネット間の自由な接続が実現され、膨大なデータ、サービスのやりとりがなされる場合、セキュリティ上の問題を考慮する必要が生じてくる。例えば、組織内部の秘密情報の外部ネットワークへの漏洩をいかに防ぐか、という問題や、組織外からの不正な侵入から、組織内ネットワークに接続された資源、情報をいかに守るか、という問題である。インターネットは、当初学術研究を目的に構築されたため、ネットワークの接続による自由なデータサービスのやりとりを重視しており、このようなセキュリティ上の問題は考慮されていなかったが、近年多くの企業、団体がインターネットに接続するようになり、セキュリティ上の問題から自組織ネットワークを防御する機構が必要となってきた。

【0005】そこで、インターネット上でデータパケットを交換する際に、外部にデータパケットを送出する前

にその内容を暗号化し認証コードをつけ、受信したサイトで認証コードを確認し復号化する、という方法がある。例えば、インターネットの標準化団体であるIETFにおいては、IPパケットの暗号化、認証コード付与方式をIPセキュリティ標準（文献：IETF RFC 1825～1829）として規定している。この方法によれば、たとえ組織外のユーザが外部ネットワーク上のデータパケットを取り出しても、内容が暗号化されているので、決してその内容が漏洩することがなく、安全な通信が確保できる。

【0006】このような暗号化通信をサポートするゲートウェイ計算機で守られた（ガードされた）ネットワーク同士であれば相互に暗号化通信が可能であり、また前述の移動計算機が自分でパケットの暗号化、復号を行う機能をサポートしていれば、任意のゲートウェイ間、またはゲートウェイ～移動計算機間で暗号化通信がサポートできる。例えば、図42では、元々ホームネットワーク1aに属していた移動計算機2が、他のネットワーク1bに移動し、ネットワーク1c内の他の計算機3（CH）と暗号化、復号機能をサポートするゲートウェイ4a、4cを介して暗号通信を行う。

【0007】一般に移動通信を行う場合、移動計算機の移動先データを管理するルータ（ホームエージェント）を置き、移動計算機宛データの送信はそのホームエージェントを経由して、移動計算機のものとのアドレス宛のIPパケットを移動IPの現在位置アドレス宛パケット内にカプセル化することで移動計算機に対するデータの経路制御を行う。図42では、ホームエージェント5（HA）がこの役割を行う。

【0008】この方式は、やはりIETFのmobile-IPワーキンググループで標準化が進められている移動IPと呼ばれる方式である（文献：IETF RFC 2003-2006）。

【0009】この移動IP方式と、先のIPセキュリティによるデータパケットの暗号化を組み合わせると、図42におけるパケットの転送経路は、CH→ゲートウェイ4c（暗号化）→ゲートウェイ4a（復号）→HA→ゲートウェイ4a（暗号化）→移動計算機2（復号）となる。

【0010】このように移動IPおよびIPセキュリティによるパケット暗号化を併用する場合、移動計算機およびその通信相手の現在位置の各場合に応じて、各構成要素の動作を変更するよう制御することが必要になる。

【0011】例えば、システムが、図1に示すような構成であるとする。ここで、MNは移動計算機、CHはその通信相手を示している。GWはパケット暗号化装置、HAはホームエージェントを示す。また、MN\*はGW（パケット暗号化認証処理）機能を自分でサポートする移動計算機である。移動計算機MNのホームドメインネットワークのことを「ホームネット」と呼ぶ。また、

「GW保護域内」とは、ゲートウェイで保護されたネットワークを指し、「GW保護域外」とは、それ以外の外部を指す。

【0012】まず、図17に示すように、MNとCHのそれぞれがGW保護域の内部か外部かで【1】～【4】の4つケースに大分類される。

【0013】なお、ここでは、CHは、固定計算機で暗号化認証処理を行わないものと仮定している。

【0014】さらに、上記の【1】【2】のGWを介した通信のケースを細分類すると、図18に示すように、(1)～(7)の7つのケースに分類される。

【0015】各々のケースについて、各ノードの処理、各GWでのIPセキュリティ処理が異なってくるので、移動IP、IPセキュリティの併用の際には、移動計算機、通信相手の位置情報をもとに、上記の【1】、【2】、(1)～(7)ケースの分類を行うことが重要になる。

【0016】また、通信相手の位置によっては、パケット暗号化を使用できない場合もある。例えば、通信相手がまったくパケット暗号化装置のない、ネットワークにいる場合である。これは、上記の【3】【4】の場合に相当する。このような場合は、移動計算機は、移動プロトコルのみを使用することになる。

【0017】また、移動IPでは、ホームエージェント経由の移動計算機宛のパケット経路を、各ネットワーク構成要素が正しい位置情報をキャッシュして保持している場合に最適化することを規定している。この経路最適化も、パケット暗号化を併用する場合、移動計算機と通信相手の現在位置を認識して、適用可能性を判定することが必要になる。

【0018】例えば、上記の(5)のケース(通信相手CHと移動計算機MNが別の部署に位置するケース)であると認識できれば、図43に示すような経路最適化が可能である。

【0019】また、移動IP方式では、移動計算機が新規の移動先に移った場合、現在位置の登録メッセージをホームエージェントに送ることが必要である。この場合も、移動計算機がホームネットワークと親しいネットワークに移動して、そのゲートウェイが登録メッセージを自由に外部に送出させる場合は、移動IPの規定のまま動作が可能だが、一般に移動計算機を外部から内部に滞在しているものとして扱うネットワークでは、セキュリティ上の考慮から、移動計算機の発するメッセージを自由に外部に送出させることは危険である。この場合、移動計算機が、自分は現在自分を侵入者として扱うネットワークにいる、ということを確認し、ゲートウェイに対して身分証明に相当する処理を行って外部アクセス許可を得た後に登録メッセージのあとの実際のデータ転送においても、ゲートウェイに対する身分証明を保持しての通信が必要である。

【0020】

【発明が解決しようとする課題】従来は、移動IP方式では、各ネットワークノードは一意的なIPアドレスが付与され、自由に制御パケットをやりとりできるという仮定で、経路制御や移動計算機位置の登録などの規定を行っていたため、実際の運用に際しては、移動計算機がどのような組織に属するネットワークに移動したか、というネットワーク運用ポリシーに関する動作規定がなく、移動IPおよびIPセキュリティによるパケット暗号化を併用する場合、移動計算機およびその通信相手の現在位置の各ケースに応じ、各移動計算機とIPパケット暗号化を行うパケット暗号化装置の動作を変更するように制御することができなかった。また、移動IPの経路最適化も困難であった。

【0021】また、移動IPの規定はネットワーク運用ポリシーを考慮していないため、例えば外部組織のネットワークに移動して移動IPの登録メッセージをホームネットワーク宛に送信する場合、外部ネットワークのゲートウェイが外向きパケットをすべて許すのであれば、移動IPの規定がそのまま使用できるが、一般にこれがセキュリティの観点から望ましくない。このため特にセキュリティを考慮し内部計算機の自由な外部アクセスを許可しないようなネットワークに移動計算機が移動した場合、移動後に行う新規位置の登録メッセージさえも移動計算機のホームネットワーク上のホームエージェントに到達させることができず、移動計算機に関する運用に障害を起こすことがあった。

【0022】本発明は、上記事情を考慮してなされたもので、相互に接続されたネットワーク間を移動して暗号通信を行うことが可能な移動計算機において、ネットワーク運用ポリシーを考慮し自装置の現在位置に応じた適正なパケット転送を行うことの可能なパケット処理装置及び通信制御方法を提供することを目的とする。

【0023】また、本発明は、上記事情を考慮してなされたもので、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機をサポートするとともに暗号通信をサポートする通信ネットワークにおいて、ネットワーク運用ポリシーを考慮しパケット通信する計算機の現在位置に応じた適正なパケット転送を行うことの可能なパケット処理装置及び通信制御方法を提供することを目的とする。

【0024】

【課題を解決するための手段】本発明(請求項1)は、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置(例えば、パケット暗号化認証処理機能を持つゲートウェイ)が設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内を移動して通信を行うことが可能な移動計算機装置であって、自装置が、自装置の移動位置情報を管理

し自装置宛のバケットを自装置の現在位置に転送する手段を有する移動計算機管理装置（例えば、ホームエージェント）の設置されたネットワークの内部に位置するか外に位置するかを認識する第1の認識手段と、自装置及び自装置が通信相手とする計算機の少なくとも一方につき、その送信するバケットを暗号化認証処理対象とするバケット処理装置が存在するか否かを認識する第2の認識手段と、これら第1及び第2の認識手段の認識結果に基づき、送信すべきバケットの暗号化認証処理を含む所定の通信処理を行う手段とを具備することを特徴とする。

【0025】暗号化認証処理を含む所定の通信処理には、例えば、バケットを暗号化せずに送信する処理、バケットの所定の通信情報を暗号化しかつ暗号通信に係る末端ノード間で行う認証のための末端認証データを付加してバケットを送信する処理、バケットの所定の通信情報を暗号化しかつ暗号通信に係る末端ノード間で行う認証のための末端認証データおよび次段のバケット処理装置との間で行う認証のための経路間認証データを付加してバケットを送信する処理が含まれる。

【0026】より具体的には、例えば、移動IPにおける、通常のIP形式のバケットを送信する処理、暗号化／末端認証形式のバケットを送信する処理、暗号化／経路間認証形式のバケットを送信する処理が含まれる。

【0027】また、移動計算機は、受信したバケットが暗号化され末端認証データが付加されている場合には、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して実際の転送データを得る。

【0028】本発明（請求項2）は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識された場合、該移動計算機管理装置へ向けて、所定の暗号化認証処理を施した、自装置の現在位置情報を含む登録メッセージを送信し、これに対し経路途中のバケット処理装置から通過拒否応答が返信された場合、該バケット処理装置の認証用鍵情報を検索し、この認証用鍵を使った認証コードを登録メッセージに付加して再送信することを特徴とする。

【0029】本発明（請求項3）は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識された場合、該ネットワークの内部の前記移動計算機管理装置へ向けて、現在位置情報を含む登録メッセージを、暗号化認証処理せずに送信することを特徴とする。

【0030】本発明（請求項4）は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理

装置の設置されたネットワークの内部に位置すると認識された場合、自装置が通信相手とする計算機に向けて、暗号化認証処理せずにバケット（例えば、通常のIP形式のバケット）を送信することを特徴とする。

【0031】本発明（請求項5）は、請求項1に記載の移動計算機装置において、前記第2の認識手段により、自装置の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在し、自装置が通信相手とする計算機の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在し、そのバケット処理装置が一致すると認識された場合、自装置が通信相手とする計算機に向けて、暗号化認証処理せずにバケット（例えば、通常のIP形式のバケット）を送信することを特徴とする。

【0032】本発明（請求項6）は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在し、自装置が通信相手とする計算機の送信するバケットを暗号化認証処理対象とする他のバケット処理装置が存在すると認識され、さらに、既に該バケット処理装置が自装置の送信するバケットを認証処理なしに外部へ通過させるものであることが判明している場合、自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データを付加されたバケット（例えば、暗号化／末端認証形式バケット）を送信することを特徴とする。

【0033】本発明（請求項7）は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在し、自装置が通信相手とする計算機の送信するバケットを暗号化認証処理対象とする他のバケット処理装置が存在すると認識され、さらに、既に該バケット処理装置が自装置の送信するバケットを認証処理なしに外部へ通過させないものであることが判明している場合、自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データおよび経路間認証データの付加されたバケット（例えば、暗号化／経路間認証形式バケット）を送信することを特徴とする。

【0034】本発明（請求項8）は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するバケットを暗号化認証処理対象とするバケット処理装



置が存在しないと認識された場合、自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データの付加されたバケット（例えば、暗号化／末端認証形式バケット）を送信することを特徴とする。

【0035】本発明（請求項9）は、請求項1に記載の移動計算機装置において、前記第2の認識手段により、自装置の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在し、自装置が通信相手とする計算機の送信するバケットを暗号化認証処理対象とするバ

ケット処理装置が存在しないと認識された場合、自装置が通信相手とする計算機に向けて、暗号化認証処理せずにバケット（例えば、通常のIP形式のバケット）を送信することを特徴とする。

【0036】また、本発明は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識され、かつ、前記第2の認識手段により、自装置が通信相手とする計算機の送信するバケットを暗号化認証処理対象とするバ

ケット処理装置が存在しないと認識された場合、自装置が通信相手とする計算機との間で、暗号通信は行わず、かつ、直接通信をすることを特徴とするようにしても良い。

【0037】また、本発明は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在し、自装置が通信相手とする計算機の送信するバ

ケットを暗号化認証処理対象とするバケット処理装置が存在しないと認識された場合、自装置が通信相手とする計算機との間で、暗号通信は行わず、かつ、自装置宛のバケットは前記移動計算機管理装置で経路制御される通信を行うことを特徴とするようにしても良い。

【0038】本発明（請求項10）は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するバケットを暗号化認証処理対象とするバ

ケット処理装置が存在し、自装置が通信相手とする計算機の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在しないと認識された場合、自装置が通信相手とする計算機との間で、暗号通信は行わず、かつ、自装置が移動先で獲得したアドレスを使用して通信相手となる計算機と直接通信することを特徴とする。

【0039】本発明（請求項11）は、請求項1に記載の移動計算機装置において、前記第1の認識手段によ

り、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在せず、自装置が通信相手とする計算機の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在しないと認識された場合、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークに対して所定の通信内容が暗号化されたバケットを送信し、該ネットワーク内のバケット転送装置（例えば、プロシキー・サーバ）によりアドレスを変換して自装置が通信相手とする計算機に転送してもらうとともに、自装置が通信相手とする計算機から送信されるバケットは、該バケット転送装置によりアドレス変換した後に、移動計算機管理装置で経路制御し、所定の通信内容を暗号化して自装置に転送してもらうことを特徴とする。

【0040】また、本発明は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識され、かつ、前記第2の認識手段により、自装置が通信相手とする計算機の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在し、該バケット処理装置が自装置を処理対象とするバケット処理装置と一致しないと認識された場合、自計算機を暗号化認証処理対象とするバケット処理装置にバケットを送信して自装置が通信相手とする計算機と暗号化通信を行い、通信相手も移動計算機宛に直接暗号化バケットを送信することを特徴とするようにしても良い。

【0041】また、本発明は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在し、自装置が通信相手とする計算機の送信するバケットを暗号化認証処理対象とするバケット処理装置が存在し、そのバケット処理装置が一致すると認識された場合（自装置の送信するバケット及び自装置が通信相手とする計算機の送信するバケットを暗号化認証処理対象とする同一のバケット処理装置が存在すると認識された場合）、自装置が通信相手とする計算機に対し、暗号化認証処理せずにデータバケットを直接送信することを特徴とするようにしても良い。

【0042】また、本発明は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するバ

ットを暗号化認証処理対象とするパケット処理装置が存在せず、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、自装置が通信相手とする計算機に対し、暗号化されかつ認証データを付与されたパケットを送信することを特徴とするようにしても良い。

【0043】また、本発明は、請求項1に記載の移動計算機装置において、前記第1の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第2の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、それらパケット処理装置が一致しないと認識された場合（自装置の送信するパケット及び自装置が通信相手とする計算機の送信するパケットを夫々暗号化認証処理対象とする同一でないパケット処理装置が存在すると認識された場合）、自装置が通信相手とする計算機に対し、通信内容が暗号化され終端間の認証データおよび自装置の移動先ネットワークに置かれたパケット処理装置との認証データを付与されたパケットを送信することを特徴とするようにしても良い。

【0044】本発明（請求項12）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有する移動計算機管理装置（例えば、ホームエージェント）の設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内に設置され、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置（例えば、暗号化認証処理機能を持つゲートウェイ）であって、転送すべきパケットの送信元となる計算機及び宛先となる計算機の少なくとも一方について、その計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機か否か（後者の場合、固定計算機またはホームネットにいる移動計算機が該当する）を認識する第1の認識手段と、前記計算機の少なくとも一方について、その計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識する第2の認識手段と、これら第1及び第2の認識手段の認識結果に基づき、前記計算機間で通信されるパケットの暗号化認証処理を含む所定の通信処理を行う手段とを具備することを特徴とする。

【0045】暗号化認証処理を含む所定の通信処理には、例えば、（a）通常の暗号化されていないパケット、（b）移動計算機管理部で経路制御され暗号化されていないパケット、（c）所定の通信情報が暗号化され

かつ暗号通信に係る末端ノード間で行う認証のための末端認証データを付加されたパケット、（d）パケットの所定の通信情報が暗号化されかつ暗号通信に係る末端ノード間で行う認証のための末端認証データおよび次段のパケット処理装置との間で行う認証のための経路間認証データを付加されたパケット、のいずれかを入力し、前記認識結果に基づいて、入力パケットを、同一のパケット形式であるいは他のパケット形式に変換して送信する処理が含まれる。

【0046】なお、上記の（a）～（d）の各々のパケット形式は、例えば、移動IPにおける、通常のIP形式、移動IP形式、暗号化／末端認証形式、暗号化／経路間認証形式である。

【0047】また、パケット処理装置は、前記認識結果に基づいて、経路最適化の可能性を判定するとともに、自装置が経路最適化に寄与するものと認識された場合、前記認識結果に応じた経路最適化のための制御を行うことができる。

【0048】本発明（請求項13）は、請求項12に記載のパケット処理装置において、前記第2の認識手段により、自装置が該移動計算機が送信するパケットを暗号化認証処理対象とすることが認識された場合、前記移動計算機から、自装置宛の経路認証データの付加されていないパケットを受信したならば、通過拒否メッセージを前記移動計算機に返信し、前記移動計算機から、自装置宛の経路間認証データの付加されたパケットを受信したならば、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段ノードに対する経路間認証データに換えて転送し、前記計算機宛の応答メッセージを受信したならば、自装置宛の経路間認証データを検査し、該経路間認証データの正当性が確認されたならば、該経路間認証データを除いて前記移動計算機に転送し、自装置が前記移動計算機管理装置の設置されたネットワークに位置する場合、前記移動計算機管理装置からの応答メッセージを受信したならば、所定の通信内容を暗号化しかつ末端認証データ及び次段ノードに対する経路間認証データを付加して該応答メッセージを前記移動計算機に宛てて転送することを特徴とする。

【0049】本発明（請求項14）は、請求項12に記載のパケット処理装置において、前記第1の認識手段により、いずれの計算機も、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機ではないと認識され、かつ、前記第1の認識手段により、いずれの計算機についても、その計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、暗号化されていないパケットが転送されて来たとき、所定の通信内容を暗号化しかつ末端認証データを付加して転送し、所定の通信内容が暗号化されかつ末端認証データを

付加されたパケットが転送されて来たとき、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号してパケットを転送することを特徴とする。

【0050】本発明（請求項15）は、請求項12に記載のパケット処理装置において、前記第1の認識手段により、少なくとも一方の計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であると認識され、前記第2の認識手段により、該一方の計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識され、かつ、前記第1の認識手段及び前記第2の認識手段により、他方の計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機ではなくかつその送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないもの、ではないと認識された場合、少なくとも転送すべき入力パケットのパケット形式に基づき、前記計算機間で通信されるパケットの暗号化認証処理を含む所定の通信処理を行うことを特徴とする。

【0051】本発明（請求項16）は、請求項15に記載のパケット処理装置において、暗号化されていないデータパケットが転送されて来た場合、所定の通信内容を暗号化しかつ末端認証データを付加して転送し、所定の通信内容が暗号化されかつ末端認証データを付加されたパケットが転送されて来た場合、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号してパケットを転送することを特徴とする。

【0052】本発明（請求項17）は、請求項15に記載のパケット処理装置において、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であって、自装置が暗号化認証処理対象とするものを送信元とする、所定の通信内容が暗号化されかつ末端認証データを付加されたパケットが転送されて来た場合、次段ノードに対する経路間認証データを付加して転送し、前記移動計算機を送信元とする、所定の通信内容が暗号化されかつ末端認証データ及び自装置に対する経路間認証データを付加されたパケットが転送されて来た場合、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段ノードに対する経路間認証データに換えて転送することを特徴とする。

【0053】本発明（請求項18）は、請求項15に記載のパケット処理装置において、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であって、自装置が暗号化認証処理対象とするものを宛先とする、所定の通信内容が暗号化されかつ末端認証データ及び自装置に対する経路間認証データを付加されたパケットが転送されて来た場

合、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送することを特徴とする。

【0054】本発明（請求項19）は、請求項15に記載のパケット処理装置において、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機でない計算機であって、自装置が暗号化認証処理対象とするものを宛先とする、所定の通信内容が暗号化されかつ自装置に対する末端認証データ及び経路間認証データを付加されたパケットが転送されて来た場合、該末端認証データ及び該経路間認証データを夫々検査し、該末端認証データ及び該経路間認証データの正当性がいずれも認識されたならば、該末端認証データ及び該経路間認証データを取り除き所定の通信内容を復号して転送することを特徴とする。

【0055】本発明（請求項20）は、請求項15に記載のパケット処理装置において、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機を宛先とし、他の計算機を送信元とするパケットであって、該移動計算機管理装置により中継されたことが示されるパケットが転送されて来た場合、該移動計算機を暗号化認証処理対象とするパケット処理装置が存在すると認識されたならば、所定の通信内容を暗号化しかつ該移動計算機に対する末端認証データ及び次段ノードに対する経路間認証データを付加してパケットを転送し、該移動計算機を暗号化認証処理対象とするパケット処理装置が存在しないと認識されたならば、所定の通信内容を暗号化しかつ該移動計算機に対する末端認証データを付加してパケットを転送することを特徴とする。

【0056】本発明（請求項21）は、請求項12、15、16または17に記載のパケット処理装置において、経路最適化を要求された際に、前記第1及び第2の認識手段による認識結果に基づいて自装置が経路最適化に寄与するものであると認識された場合、前記認識結果に応じた所定の経路最適化処理を行うことを特徴とする。

【0057】また、本発明は、請求項12に記載のパケット処理装置において、前記第1及び第2の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識され、かつ、移動計算機及び移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、前段で移動計算機が送信した、所定の通信内容が暗号化されかつ末端認証データ及び前段との経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認

証データを次段に対するものに換えて転送し、次段が移動計算機である、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送し、それ以外の、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該末端認証データ及び該経路間認証データを夫々検査し、該末端認証データ及び該経路間認証データの正当性がいずれも認識されたならば、該末端認証データ及び該経路間認証データを取り除き所定の通信内容を復号して転送し、移動計算機管理部で経路制御され、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データ及び次段に対する経路間認証データを付与して転送することを特徴とするようにしても良い。

【0058】また、本発明は、請求項12に記載のパケット処理装置において、前記第1及び第2の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが該移動計算機と同じネットワークに位置すると認識され、かつ、移動計算機及び移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送し、所定の通信内容が暗号化されかつ末端認証データが付与されたパケットを受信したら、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して転送し、移動計算機管理部で経路制御され、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データ及び次段に対する経路間認証データを付与して転送し、次段が移動計算機である、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送することを特徴とするようにしても良い。

【0059】また、本発明は、請求項12に記載のパケット処理装置において、前記第1及び第2の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが該移動計算機と同じネットワークに位置すると認識され、かつ、移動計算機及び移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、移動計算機に対するデータ転送経路の最適化が要求され、前記第2の認識手段により、自装置が通

信相手計算機が送信するパケットを暗号化認証処理対象とすることが認識されたとき、通信相手計算機からの暗号化されていないパケットを受信したら、該パケットを移動計算機管理装置で経路制御されたものと同じ形式のパケットに変換して移動計算機に転送することを特徴とするようにしても良い。

【0060】また、本発明は、請求項12に記載のパケット処理装置において、前記第1及び第2の認識手段により、移動計算機が前記移動計算機管理装置の設置された第1のネットワークの外に位置し、移動計算機が通信相手とする固定ノードが該移動計算機と異なるネットワークでかつ第1のネットワークでないネットワークに位置すると認識され、かつ、前記第2の認識手段により、移動計算機及び移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送し、所定の通信内容が暗号化されかつ末端認証データが付与されたパケットを受信したら、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して転送し、前段で移動計算機が送信した、所定の通信内容が暗号化されかつ末端認証データ及び前段との経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送し、それ以外の、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該末端認証データ及び該経路間認証データを夫々検査し、該末端認証データ及び該経路間認証データの正当性がいずれも認識されたならば、該末端認証データ及び該経路間認証データを取り除き所定の通信内容を復号して転送し、移動計算機管理部で経路制御され、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データ及び次段に対する経路間認証データを付与して転送することを特徴とするようにしても良い。

【0061】また、本発明は、請求項12に記載のパケット処理装置において、前記第1及び第2の認識手段により、移動計算機が前記移動計算機管理装置の設置された第1のネットワークの外に位置し、移動計算機が通信相手とする固定ノードが該移動計算機と異なるネットワークでかつ第1のネットワークでないネットワークに位置すると認識され、かつ、前記第2の認識手段により、

移動計算機及び移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合であって、かつ、移動計算機に対するデータ転送経路の最適化が要求された場合、前記第2の認識手段により、自装置が移動計算機が送信するパケットを暗号化認証処理対象とすることが認識されたとき、前段で移動計算機が送信した、所定の通信内容が暗号化されかつ末端認証データ及び前段との経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段に対するものに換えて転送し、次段が移動計算機である、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送し、前記第2の認識手段により、自装置が通信相手計算機が送信するパケットを暗号化認証処理対象とすることが認識されたとき、次段が通信相手計算機である、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該末端認証データ及び該経路間認証データを夫々検査し、該末端認証データ及び該経路間認証データの正当性がいずれも認識されたならば、該末端認証データ及び該経路間認証データを取り除き所定の通信内容を復号して転送し、前段で通信相手計算機が送信した、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データ及び経路間認証データを付与して移動計算機に転送することを特徴とするようにしても良い。

【0062】また、本発明は、請求項12に記載のパケット処理装置において、前記第1及び第2の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識され、かつ、移動計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在せず、移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、所定の通信内容が暗号化されかつ末端認証データを付与されたパケットを受信したら、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して転送し、移動計算機管理部で経路制御され、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送することを特徴とするようにしても良い。

【0063】また、本発明は、請求項12に記載のパケット処理装置において、前記第1及び第2の認識手段に

より、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、移動計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在せず、移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送し、所定の通信内容が暗号化されかつ末端認証データが付与されたパケットを受信したら、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して転送し、移動計算機管理部で経路制御され、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送することを特徴とするようにしても良い。

【0064】また、本発明は、請求項12に記載のパケット処理装置において、前記第1及び第2の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、移動計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在せず、移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合であって、かつ、移動計算機に対するデータ転送経路の最適化が要求された場合、前記第2の認識手段により、自装置が通信相手計算機が送信するパケットを暗号化認証処理対象とすることが認識されたとき、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送し、前段で通信相手計算機が送信した、所定の通信内容が暗号化されかつ末端認証データが付与されたパケットを受信したら、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して転送して移動計算機に転送することを特徴とするようにしても良い。

【0065】本発明（請求項22）は、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置が設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内を移動して通信を行うことが可能な移動計算機装置の通信制御方法であって、自装置が、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークの内部に位置するか外に位置するかを認識するとともに、自

装置及び自装置が通信相手とする計算機の少なくとも一方につき、その送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識し、これら認識結果に基づき、送信すべきパケットの暗号化認証処理を含む所定の通信処理を行うことを特徴とする。

【0066】本発明（請求項23）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内に設置され、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置の通信制御方法であって、転送すべきパケットの送信元となる計算機及び宛先となる計算機の少なくとも一方について、その計算機が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機か否か（固定ノードまたはホームネットにいる移動計算機）を認識し、前記計算機の少なくとも一方について、その計算機が送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識し、これら認識結果に基づき、前記計算機間で通信されるパケットの暗号化認証処理を含む所定の通信処理を行うことを特徴とする。

【0067】従来、移動IP方式では、各ネットワークノードは一意なIPアドレスが付与され、自由に制御パケットをやりとりできるという仮定でのみ、経路制御や移動計算機位置の登録などの規定を行っていたが、本発明によれば、実際の運用に再して、移動計算機がどのような組織に属するネットワークに移動したか、というネットワーク運用ポリシーに関する動作規定、例えば暗号通信するか否か、認証を必要とするか否かなどを考慮することができる。

【0068】また、IPセキュリティにもとづく暗号化装置を介して暗号化、認証通信を行う場合、各移動計算機およびその通信相手の位置に応じて各ネットワーク構成要素の動作が大きく変化する。特に、暗号化認証処理をともなつて、移動IPの経路最適化を行うためにも、この位置情報認識を有効に利用できる。

【0069】また、移動IPの規定は、ネットワーク運用ポリシーを考慮していないため、例えば、外部組織のネットワークに移動して移動IPの登録メッセージをホームネットワーク宛に送信する場合、外部ネットワークのゲートウェイが外向きパケットをすべて許すのであれば、移動IPの規定がそのまま使用できるが、一般にこれはセキュリティの観点から望ましくない。したがって、移動計算機は、自身が外部組織のネットワークにいる、ということを確認し、ゲートウェイに対して自分の身分証明を行う処理を行ってから外部アクセスを行うことが必要になるが、本発明によれば、移動計算機が自身

の現在位置を認識して現在接続しているネットワークから外へのアクセスを行う場合に必要な処理を正しく実行できる。

【0070】以上のように本発明によれば、例えば移動IPによる移動計算機の制御とIPセキュリティによるパケット暗号化処理をあわせて適用した場合に、実際のシステムで運用する場合の各ネットワークの管理ポリシーを反映しかつ効率の良いシステム制御を実現できる。すなわち、本発明によれば、システム全体のネットワーク構成に依存せずに移動計算機制御方式とパケット暗号化方式の両者を適用した通信システムを実現できる。

【0071】なお、以上の各装置に係る発明は、方法に係る説明としても成立する。

【0072】また、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【0073】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0074】通信システム内を移動して通信を行うことが可能な計算機を移動計算機と呼び、通信システム内を移動せず固定の位置で通信を行う計算機を固定計算機と呼ぶ。

【0075】ある移動計算機について、その移動計算機がホームポジションを持つネットワークのことをホームネットワークと呼び、ホームネットワーク以外のゲートウェイを有するネットワークを他部署ネットワークと呼ぶ。

【0076】ホームネット内にいる（本来の位置の他に、ホームネット内で単にルータを越えた移動はしているが、ゲートウェイを越えた移動はしていない場合を含む）移動計算機は、固定計算機と同様の扱いとなる。

【0077】固定ノードは、ホームネット内にいる移動計算機と固定計算機を含む。

【0078】また、GW保護域内とは、ゲートウェイで保護されているネットワーク（図1では、ホームネットワーク、他部署ネットワーク）を指す。GW保護域外とは、それ以外の外部を指す。後者の場合の計算機を外部ノードと呼ぶ。

【0079】図1に、本実施形態に係る通信システムの基本構成の一例を示す。

【0080】図1の通信システムは、先に図42や図43を参照しながら説明した移動IP、IPセキュリティなどにより移動計算機の通信をサポートしているものとする。なお、移動IPプロトコルでは、移動先ネットワークで移動計算機に対するパケット配送を行うフォーリンエージェントというルータの存在を仮定するモードと、フォーリンエージェントを設けない（移動先計算機自身がフォーリンエージェントを兼ねる）ポップアップモードがあるが、本実施形態では、ポップアップモード



を採用するものとして説明する。

【0081】ところで、計算機間のパケット通信には、固定計算機間の通信、固定計算機・移動計算機間の通信、移動計算機間の通信の3つのケースが存在し得る。そして、ホームネット内に位置する移動計算機は固定ノードであるので、計算機間のパケット通信は、固定ノード間の通信、固定ノード・ホームネット外に移動中の移動計算機間の通信、ホームネット外に移動中の移動計算機間の通信の3つに分類できる。

【0082】固定計算機間の通信と、固定計算機・ホームネット内に位置する移動計算機間の通信と、ホームネット内に位置する移動計算機間の通信とは、いずれも同様の制御手順となる。また、ホームネット外に移動中の移動計算機間の通信は、経路最適化前は固定ノードであるホームエージェントを介した通信になるので、ホームネット外に移動中の移動計算機と固定計算機との間の通信に帰結される。

【0083】従って、本実施形態では、移動計算機(MN)2・通信相手計算機(CH)の間でのパケット転送について、通信相手計算機(CH)3を固定ノードとした場合を中心に説明し、その他に通信相手計算機(CH)3を移動計算機とした場合や固定計算機同士の通信について言及する。

【0084】なお、本実施形態では、図1のネットワーク1aの内部にホームポジションを持つ移動計算機(MN)2とその通信相手計算機(CH)3に関するパケット通信を中心にして説明を行うので、図1では、ネットワーク1aをホームネットワーク、ネットワーク1b、1cを他部署ホームネットワークとして示してある。

【0085】さて、図1では、ホームネットワーク1a、第1の他部署ネットワーク1b、第2の他部署ネットワーク1cがインターネット6を介して相互に接続されており、移動計算機(MN)2、移動計算機の通信相手(CH)3は、これらネットワーク内に接続され、または外部ノードとしてインターネット6に接続される。ネットワーク1a、1b、1cには、入力パケットに所定のパケット処理を施して転送するパケット処理装置(すなわちパケット暗号化ゲートウェイ;以下ゲートウェイと呼ぶ;また、GWはゲートウェイを表すものとする)4a、4b、4cがそれぞれ設けられるものとする。ゲートウェイ4a、4b、4cは、所定のセキュリティポリシーに従ってフィルタリングも行うが、本実施形態では、パケットが各ゲートウェイの通過条件を満たす場合について説明する(通過条件を満たさない場合はそのゲートウェイを通過できないだけである)。

【0086】ホームネットワーク1aには、移動IPプロトコルをサポートするために、移動計算機の移動先の現在位置の情報を管理するホームエージェント(HA)5aが設けられる。管理対象とする移動計算機の台数は任意である。前述したように、移動中の移動計算機2宛

に転送されてきたIPパケットは、そのホームエージェント5を経由し、移動計算機2の元のアドレス(ホームネットワーク1aにおけるアドレス)宛のIPパケットを移動IPの現在位置アドレス宛パケット内にカプセル化することで、移動計算機2に対するデータの経路制御を行うことができる。なお、第1の他部署ネットワーク1b、第2の他部署ネットワーク1cにも、必要に応じて、ホームエージェント5b、5cが設けられる。また、後述する第3の他部署ネットワーク1dにも、同様の機能を持つホームエージェント5dが設けられる。

【0087】本実施形態では、ゲートウェイ4a、4b、4cは、パケット暗号化認証処理機能を持つものとする。また、移動計算機2は、少なくとも移動中には、パケット暗号化認証処理機能を持つものとする(図中、パケット暗号化認証処理機能を持つ移動計算機2をMN+で表す)。なお、パケット暗号化認証処理における通信データの暗号化/復号は、例えば、文献(IETF RFC1825, 1827)に示される方式で実現できる。また、パケット暗号化認証処理における、認証データ(転送パケット内容と生成鍵から生成されるハッシュ関数値など)の付与/チェックは、例えば、文献(IETF RFC1825, 1826)に示される方式で実現できる。

【0088】なお、本実施形態では、固定計算機(特に外部ノードである固定計算機)はパケット暗号化認証処理機能を持たないものとして説明する(外部ノードである固定計算機がパケット暗号化認証処理機能を持つ場合については後に言及する)。

【0089】本実施形態では、暗号/移動通信をサポートするため、パケット通信する計算機の位置、ゲートウェイの位置などに応じて、種々のフォーマットを持つパケット形式が使用される。

【0090】図2に、ゲートウェイ、移動計算機で処理されるパケット形式を示す。

【0091】(a)は、通常のIPパケット形式である。

【0092】IPヘッダには、通信を行う計算機の送信元のホーム・アドレスと宛先のホーム・アドレスが書込まれる。本実施形態では、IPヘッダには、送信元となる計算機のアドレスと宛先となる移動計算機のアドレスが書込まれるものとする。

【0093】(b)は、移動IP形式であり、ホームエージェントで移動計算機宛に経路制御されるパケット形式である。

【0094】先頭のIPヘッダには、送信元としてホームエージェントのアドレス、宛先として移動計算機の現在位置のケア・オブ・アドレス(Care-ofアドレス)が書込まれ、後続のIPヘッダには、送信元となる計算機のアドレスと宛先となる移動計算機のホーム・アドレス(プライベート・アドレス(Privateアド

レス))が書込まれるものとする。

【0095】(c)は、暗号化/末端認証形式であり、末端のゲートウェイ間または末端のゲートウェイ〜移動計算機間でパケットの暗号化および認証を行う形式である。

【0096】末端間認証/暗号化情報のIPヘッダには、暗号化/認証を行う末端ノードの送信元アドレスと宛先アドレスが書込まれる。

【0097】KEY情報(鍵情報ヘッダ)は、受信側が認証処理に使用する鍵と復号処理に使用する鍵を得るための情報を含むヘッダ情報である。例えば、上記鍵をパケット処理鍵から生成する場合、IPヘッダの送信元ノードと宛先ノードとの間で共有されるマスター鍵で暗号化されたパケット処理鍵が書込まれる。その他、必要に応じて、認証アルゴリズム、データの暗号化アルゴリズム、鍵暗号アルゴリズムを指定するための情報が書込まれる。

【0098】AH情報(認証ヘッダ)は、所定の鍵(例えば、上記パケット生成鍵から生成した認証鍵)を使って生成された認証データを含むヘッダ情報である。

【0099】ESP情報(暗号化ヘッダ)は、所定の鍵(例えば、上記パケット生成鍵から生成した暗号鍵)を使って暗号化された内部データ(ここでは、内部IPヘッダとそのデータ部)を復号するアルゴリズムを指定する情報を含むヘッダ情報である。

【0100】内部IPプロトコルは、カプセル化されたパケットであり、通信を行う計算機の送信元アドレスと宛先アドレスを含む内部IPヘッダやそのデータ部からなる。例えば、上記(a)のパケットや上記(b)のパケットに該当する。

【0101】(d)は、暗号化/経路間認証形式である。途中経路間でのゲートウェイ間、途中経路のゲートウェイ〜移動計算機間の認証を必要とする場合にはこの形式を使用する。

【0102】末端間認証/暗号化情報の部分、内部プロトコルの部分は、上記(c)の場合と同様である。

【0103】経路間認証情報のIPヘッダには、認証を行うノードの送信元アドレスと宛先アドレスが書込まれる。

【0104】KEY情報(鍵情報ヘッダ)は、受信側が認証処理に使用する鍵を得るための情報を含むヘッダ情報である。例えば、上記と同様、上記鍵をパケット処理鍵から生成する場合、IPヘッダの送信元ノードと宛先ノードとの間で共有されるマスター鍵で暗号化されたパケット処理鍵が書込まれ、その他、必要に応じて、認証アルゴリズム、鍵暗号アルゴリズムを指定するための情報が書込まれる。

【0105】AH情報(認証ヘッダ)は、所定の鍵(例えば、上記パケット生成鍵から生成した認証鍵)を使って生成された認証データを含むヘッダ情報である。

【0106】なお、(c)の暗号化/末端認証形式と、(d)の暗号化/経路間認証形式では、いずれかの平文のヘッダ内に、送信元計算機のアドレスの情報と宛先計算機のアドレスの情報とを書込んで置くのが望ましい。

【0107】また、ゲートウェイ、移動計算機が使用する認証データとして、例えば、転送パケット内容と生成鍵から生成される一方ハッシュ関数値(例えば、Keyed MD5方式)などが利用できる。

【0108】また、2つのデータパケット暗号化装置間あるいはデータパケット暗号化装置と移動計算機の間で共有されるマスター鍵は、例えば、秘密鍵の交換や、公開鍵と秘密鍵による導出(例えば、Diffie-Hellman法)により生成することができる。

【0109】末端間での認証は、固定ノードを暗号化認証処理対象とするゲートウェイ間、移動計算機のホームネットのゲートウェイと、ホームネット外に移動中の当該移動計算機との間で行われる。

【0110】経路間の認証は、ゲートウェイを持つ他のネットワークに移動中の移動計算機と当該移動計算機のホームネット内のノードとの通信において当該計算機のホームネットのゲートウェイと当該計算機の移動先ネットのゲートウェイとの間、および当該移動計算機の送信するパケットをその移動先ネットのゲートウェイが認証なしに外部へ通過させない場合に当該移動計算機とその移動先ネットのゲートウェイ間で行われる。

【0111】各ゲートウェイは、上記のいずれかの形式で入力されたパケットを、同一形式あるいは形式を変換して転送する。その際、自装置が末端認証や経路間認証の宛先になっている場合には、認証チェックに成功した場合のみパケットを通過させる。また、自装置が末端認証や経路間認証の送信元になっている場合には、所定のヘッダ情報を付加し、あるいは所定のヘッダ情報を付け替えて送信する。なお、パケット転送にあたっては、必要に応じて内部データの復号/再暗号化を行う。

【0112】また、各計算機は、上記の移動IP形式以外のいずれかの形式でパケットを送信し、上記のいずれかの形式でパケットを受信する。自装置が末端認証の宛先になっている場合には、内部データの復号を行うとともに、認証チェックに成功した場合のみ内部データを受け入れる(例えば上位モジュールに渡す)。また、移動IP形式のパケットについては、デカプセル化を行う。

【0113】移動IP形式のパケットを転送するのは、基本的にはホームエージェントだけである(なお、後述する経路最適化の特殊なケースとしてゲートウェイの場合もある)。

【0114】次に、本実施形態では、ゲートウェイ4a、4b、4cは、自装置が現在、暗号化認証処理対象とする計算機を認識する暗号化認証処理対象計算機認識部を持つ。例えば、通信システム内のいずれかの場所(分散していても良い)に、各ゲートウェイがどの計算



機を暗号化認証処理対象とするかを示す情報のデータベース（具体例としては各ゲートウェイのネットワークアドレスと、その暗号化認証処理対象となる計算機群のネットワークアドレスの対応情報）を管理するサーバ装置を設置し、移動計算機が該データベースを検索することにより実現できる。あるいは、各ゲートウェイが、自装置の暗号化認証処理対象となる計算機群のネットワークアドレスの情報を保持することで実現できる。

【0115】また、各移動計算機は、後述する位置認識部により上記データベースやゲートウェイへの問い合わせなどを行うことにより、現在、自装置を暗号化認証処理対象とするゲートウェイを検索することができる。

【0116】また、本実施形態では、各ゲートウェイ4a、4b、4cは、上記の暗号化認証処理対象計算機認識部の他に、自装置が管理対象とする送信元計算機を認識する管理対象計算機認識部を持つ。管理対象計算機認識部は、例えば、通信システム内のいずれかの場所（分散していても良い）に、各ゲートウェイがどの計算機を管理対象とするかを示す情報のデータベース（具体例としては各ゲートウェイのネットワークアドレスと、その管理対象となる計算機群のネットワークアドレスの対応情報）を管理するサーバ装置を設置し、移動計算機が該データベースを検索することにより実現できる。あるいは、各ゲートウェイが、自装置の管理対象となる計算機群のネットワークアドレスの情報を保持することで実現できる。

【0117】ゲートウェイ4a、4b、4cは、ネットワーク内部の計算機から送信されたバケットが自装置の管理する計算機（例えば、当該ネットワーク内部をホームポジションとする計算機）から送信されたものである場合は、該バケットを認証チェックなしに（必要な処理を施した上で）外部へ通過させ、該バケットが自装置の管理しない計算機（例えば、一時的にそのネットワーク内に移動してきた計算機）から送信されたものである場合は、該バケット内に正当な認証データが含まれれば該バケットに必要な処理を施した上で通過させるが、該バケット内に正当な認証データが含まれなければ（該バケット内に認証データが含まれるが認証チェックで正当でないものと判断された場合、あるいは該バケット内に認証データ自体が含まれない場合）、該バケットの外部への通過を拒否する。

【0118】また、ゲートウェイ4a、4b、4cは、バケットの転送を拒否された計算機から認証データを生成するために必要な鍵の情報を要求された場合には、要求メッセージから求められる該移動計算機のユーザに関する情報が所定の条件を満たすことを確認したならば、要求された鍵情報を返送する。

【0119】なお、ネットワークによっては、そのセキュリティポリシーに応じ、外部から移動してきた計算機の送信したバケットを認証チェックなしに外部へ通過さ

せる場合も存在し得る。例えば、親しいネットワークから移動してきた移動計算機など、所定のものに限って管理対象として登録している場合、ネットワーク内部の計算機から送信されたバケットが自装置の管理する計算機から送信されたものか否かにかかわらず認証チェックなしに外部へ通過させる場合などが考えられる。

【0120】もし、あるネットワークにおいてネットワーク内部から認証チェックなしにすべてのバケットを外部へ通過させるセキュリティポリシーを採用する場合、そのネットワークのゲートウェイでは管理対象計算機認識部は不要となる。

【0121】以下では、移動計算機2が他部署ネットワーク1bに移動した場合に行われる処理について説明する。

【0122】まず、移動計算機2自身による現在位置検出、移動先ネットワークで使用するケア・オブ・アドレスの獲得などについて説明する。

【0123】移動計算機2は、自装置を管理するホームエージェント5aの設置されたネットワーク（ホームネットワーク）1a外に位置することを認識する位置認識部を持つ。

【0124】図3に、位置認識部により移動計算機2の現在位置を検出する処理手順の一例を示す。

【0125】ここで、移動IPの規定にあるように各ホームエージェントはその処理するサブネット内に定期的にエージェント広告メッセージをブロードキャストにより送出するものとする。また、各ゲートウェイは、各々が検査対象とする計算機のアドレスのリストを公開しており、ある計算機について、その送信バケットのチェックを司るゲートウェイを検索可能であるとする。

【0126】移動計算機2側では、まず、自装置がホームネットワーク1aの内部に位置するか外に位置するかを判定する。自装置を管理するホームエージェント5aの送出するエージェント広告メッセージを受信し、ホームネットワーク内部に位置するか外に位置するかを検知する。自装置の属するホームネットワーク1aのホームエージェント5aによるエージェント広告メッセージを受信した場合にはホームネットワーク1a内部に位置すると判定する。それ以外のホームエージェントによるエージェント広告メッセージを受信した場合、あるいはエージェント広告メッセージを受信できない場合にはホームネットワークの外に位置すると判定する（ステップS11）。

【0127】移動計算機2は、自装置がホームネットワークの外に位置すると判定された場合（ステップS12）、移動先のネットワーク（ここでは1b）において、例えばDHCPやPPPなどのプロトコルにより、移動先ネットワークで使用する移動IPのケア・オブ・アドレスを取得する（ステップS13）。

【0128】さらに、移動計算機2は、そのケア・オブ

・アドレスを保護する(暗号化認証処理対象とする)ゲートウェイ(GW\_MH)を検索する(ステップS14)。

【0129】ここで、検索されたゲートウェイ(GW\_MH)とホームネットワークのゲートウェイが一致している場合(例えばホームネットワーク1a内で他のサブネットに移動した場合)には、自装置はホームドメイン内に位置すると判定する[MN-home]。そうでない場合には、ホームドメイン外に位置すると判定する[MN-foreign]。

【0130】なお、ホームドメイン内に位置すると判定された場合には、以下に示す一連の位置登録処理は実行せず、通常のIPパケット形式で登録要求を送る。

【0131】また、ケア・オブ・アドレスを保護するゲートウェイが存在しない場合、移動計算機2は外部ノードである。

【0132】なお、ケア・オブ・アドレスを取得した時点で、移動計算機2と、これを暗号化認証処理対象とするゲートウェイとの対応付けが所定のデータベース等に登録される。

【0133】次に、移動計算機がホームエージェントへ移動登録メッセージを通知する処理について説明する。

【0134】移動IP方式では、移動計算機が新規の移動先に移った場合、現在位置の情報を含む登録メッセージを、自装置を管理するホームエージェントに送ることが必要である。この場合、移動計算機がホームネットワークと親しいネットワークに移動して、そのゲートウェイが自装置の送信する登録メッセージやデータパケットを自由に外部に送出させる場合には、移動IPの規定のままで動作が可能である。しかし、一般に移動計算機を外部から内部に滞在しているものとして扱うネットワークでは、セキュリティ上の考慮から、移動計算機の発するメッセージを自由に外部に送出させることは危険であることから、ゲートウェイは自装置が管理対象とする計算機以外の移動計算機の送信する登録メッセージやデータパケットを一旦通過拒否する。このような場合、移動計算機は、現在自装置を侵入者として扱うネットワークに位置することを認識し、そのゲートウェイとの間で身分証明に相当する手続きを行って外部アクセス許可を得た後に登録メッセージをホームエージェントへ送信することが必要になる。

【0135】IETFではIPパケットへの認証コード付与方式をIPセキュリティ標準(文献:IETF RFC1826, 1828)として規定しているが、この方法を利用し、移動計算機の身分証明のための処理としてデータパケットに移動計算機と移動先ネットワークのゲートウェイ間での認証データを付加し、ゲートウェイでは受信したパケットの認証コードを確認してから、外部にパケットを通過させるようにする。これによって、たとえ組織外のユーザが入って来てネットワーク外部に

対しデータパケットを送信したいと要求しても、予め所定の方法で認証鍵を交換し身分保証を行った移動計算機のみ外部アクセスを許可することが可能となる。

【0136】さて、移動計算機2は、ケア・オブ・アドレスを獲得したら、ホームネットワーク1aのホームエージェント5aに現在位置の情報を含む登録メッセージを送信する。

【0137】まず、移動計算機2がホームドメインにいる[MN-home]の場合は、

- 10 ・ホームエージェント(HA)のIPアドレス
- ・移動計算機(MN)のIPアドレス

を調べ、移動計算機を送信元、ホームエージェントを宛先とする通通常IPパケット形式で登録要求を送り、ホームエージェントからのIPパケット形式の応答を受信するだけでよい。

【0138】なお、ここでは、ホームエージェントと移動計算機のIPアドレスは、ホームネットでのプライベート・アドレスとする。

- 20 【0139】次に、移動計算機2がホームドメイン外[MN-foreign]に移動している場合について説明する。

【0140】移動計算機2がホームドメイン外[MN-foreign]に移動している場合(図4)、まず、

- ・ホームネットワークのゲートウェイ(GW0)のglobalアドレス
- ・ホームネットワークのゲートウェイ(GW0)の公開鍵

・移動計算機(MN)のケア・オブ・アドレス、プライベート・アドレス

- 30 ・ホームエージェント(HA)のプライベート・アドレス

を調べ、第1の登録メッセージを送る。

【0141】図5に第1の登録メッセージの一例を示す。

【0142】このメッセージは、前述した図2(c)の暗号化/末端認証形式のパケットに該当する。

【0143】末端間認証/暗号化情報のIPヘッダでは、送信元を移動計算機(MN)2のケア・オブ・アドレス、宛先をゲートウェイ(GW0)4aのグローバル・アドレスとする。

【0144】内部IPヘッダ(登録要求)では、送信元を移動計算機(MN)のプライベート・アドレス、宛先をホームエージェント(HA)のプライベート・アドレスとする。

【0145】これに対し、移動計算機2がホームネットワーク1aと親しいネットワークに移動して、そのゲートウェイが登録メッセージを自由に外部に送出させるような場合には、ゲートウェイ4bは認証チェックなしに登録メッセージを通過させるので、ゲートウェイ4bから移動計算機2へ受諾応答が返されるだけであるが、も

しゲートウェイ4bが、管理対象でない計算機から装置宛でないパケットを受信したならば外部へのパケットの通過を拒否するような場合には、この登録メッセージの通過は拒否され、ゲートウェイ4bから移動計算機2へ通過拒否メッセージが返送される。

【0146】図6に、通過拒否メッセージの一例として、TCP/IP通信のICMPメッセージを拡張した形式で実現したものを示す。

【0147】このメッセージは、前述した図2(a)の通常のIPパケット形式に該当する。

【0148】IPヘッダでは、送信元をゲートウェイ4b(GW1)のグローバル・アドレス、宛先を移動計算機(MN)のケア・オブ・アドレスとする。

【0149】この場合は、移動計算機2は、通過拒否メッセージ中に含まれるゲートウェイ4bのグローバル・アドレスを用いて、ゲートウェイ4bに対し鍵要求メッセージを送信して、所定のプロトコルにより公開鍵の問い合わせを行う。

【0150】図7に、鍵要求メッセージの一例を示す。

【0151】このメッセージは、前述した図2(a)の通常のIPパケット形式に該当する。

【0152】IPヘッダでは、送信元を移動計算機(MN)のケア・オブ・アドレス、宛先をゲートウェイ4b(GW1)のグローバル・アドレスとする。

【0153】この鍵要求メッセージに対し、ゲートウェイ4bが公開鍵情報を渡すか否かの判断は、ゲートウェイ4bのサイトのシステム管理のポリシーに依存する。

【0154】例えば、

- ・鍵要求情報に所定の書式で付加されたユーザ識別情報を調べ、社内ユーザであれば、鍵情報を返す。
- ・社外ユーザであれば、所定の組織であれば鍵情報を渡す。
- ・それ以外の場合、予め登録されたユーザであれば、鍵情報を渡す。

といった規則をゲートウェイ4bに登録しておく。

【0155】ゲートウェイ4bに対するユーザ登録方法などはシステムの性質に応じ任意に設定すれば良い。

【0156】この鍵要求メッセージに対し、ゲートウェイ4bの公開鍵が得られたら、移動計算機2は、この鍵を使って生成した認証データを付加した2度目の登録要求を送る(なお、ゲートウェイ4bの管理対象でない計算機が、鍵情報を入手できなければ、この計算機は、ゲートウェイ4bから外にパケットを通過させることはできない)。

【0157】図8に、第2の登録メッセージの一例を示す。

【0158】このメッセージは、前述した図2(d)の暗号化/経路間認証形式のパケットに該当する。

【0159】経路間認証情報のIPヘッダ1では、送信元を移動計算機(MN)2のケア・オブ・アドレス、宛

先をゲートウェイ(GW1)4bのグローバル・アドレスとする。

【0160】末端間認証/暗号化情報のIPヘッダ2では、送信元を移動計算機(MN)2のケア・オブ・アドレス、宛先をゲートウェイ(GW0)4aのグローバル・アドレスとする。

【0161】内部IPヘッダ(登録要求)では、送信元を移動計算機(MN)のプライベート・アドレス、宛先をホームエージェント(HA)のプライベート・アドレスとする。

【0162】この第2の登録メッセージには、ゲートウェイ4b宛でかつゲートウェイ4bに対する認証データを含むAH情報(図2(d)の経路間認証情報中のAH情報)が付与されているので、ゲートウェイ4bは認証チェック処理を行い、これに成功すればメッセージは通過できる。

【0163】その際、ゲートウェイ4bは、次段のゲートウェイ4a宛に、図2(d)の暗号化/経路間認証形式パケットで登録メッセージを転送する。

【0164】そして、登録メッセージは、インターネット6からゲートウェイ4aを介してホームエージェント5aに到着する。

【0165】登録メッセージが移動計算機2のホームネットワーク1aのホームエージェント5aに到着すると、その管理表には、移動計算機2の全ネットワーク中における位置を一意に特定可能な情報が登録される(この時点で、ホームエージェント5aは、移動計算機2がホームネットワーク1a外に移動したことを認識する)。

【0166】また、例えば、ネットワーク1aでは、ゲートウェイ4bの管理表に、インターネット6側からその移動計算機2宛に転送されてきたパケットをホームエージェント5aに転送するように設定がなされる。これによって、インターネット6から移動計算機2のホームネットワーク1aに転送されてきた移動計算機2宛のパケットは、一旦ホームエージェント5aに渡され、ここから、移動計算機2の移動先に宛てて転送されるようになる。その際、ホームエージェント5aにて、前述したように、移動計算機2の元のアドレス(ホームネットワーク1aにおけるアドレス)宛のIPパケットを移動IP形式の現在位置アドレス宛パケット内にカプセル化する処理が行われる。あるいは、ホームエージェントがMNのproxy ARPを行って、パケットを取るようにしても良い。

【0167】さて、登録メッセージを受けたホームエージェント5aは、移動計算機2に対して、ホームエージェント5aを送信元、移動計算機2を宛先とするIP形式の登録応答メッセージを送信する。

【0168】ホームエージェント5aから登録応答メッセージを受信すると、ゲートウェイ4aは、このパケッ

トを図9に示すように次段のゲートウェイ4b宛の暗号化／経路間認証形式にカプセル化して転送する。

【0169】経路間認証情報のIPヘッダ1では、送信元をゲートウェイ4a (GW0) のグローバル・アドレス、宛先をゲートウェイ4b (GW1) のグローバル・アドレスとする。

【0170】末端間認証／暗号化情報のIPヘッダ2では、送信元をゲートウェイ4a (GW0) のグローバル・IPアドレス、宛先を移動計算機(MN) のケア・オブ・アドレスとする。

【0171】内部IPヘッダ(登録要求)では、送信元をホームエージェント(HA) のプライベート・アドレス、宛先を移動計算機(MN) のプライベート・アドレスとする。

【0172】このパケットがゲートウェイ4bに到達すると、ゲートウェイ4bでは、図10に示すように暗号化／末端認証形式にして(IPヘッダ1、KEY1、AHを取り除いて) 移動計算機宛に転送する。

【0173】以上の登録処理が完了したら(登録メッセージに対して一旦転送拒否を示すメッセージを受信した後に鍵情報と認証データのやり取りによって応答承諾を受信した場合)、それ以降、移動計算機2がその移動中のネットワークの外部に位置する通信相手計算機3とデータ通信を行う場合も、上記の移動計算機2へゲートウェイ4b間の認証データをパケットに付加して転送する。本実施形態では、暗号化／経路間認証形式でパケットを送信する。この認証データ付加があるか否かによって、ゲートウェイ4bにて正しく認識されている訪問ノードであるか否かを正しく判定し、セキュリティに正しい移動計算機のメッセージ制御を行うことが可能となる。

【0174】なお、登録メッセージに対して転送拒否されずに応答承諾を受けた場合には、通信相手となる計算機3へのパケットを通常通り送信する。本実施形態では、暗号化／末端認証形式でパケットを送信する。

【0175】なお、移動計算機が外部ノードとして移動した場合には、移動計算機からホームエージェントへの登録メッセージは暗号化／末端認証形式で送信され、上記と異なり通過拒否なしにゲートウェイに転送され、ここでIP形式にされホームエージェントに到達する。また、ホームエージェントから移動計算機への通常のIP形式の応答メッセージはゲートウェイで暗号化／末端認証形式に変換され、移動計算機に到達する。以降、移動計算機2がその通信相手計算機3とデータ通信を行う場合も、暗号化／末端認証形式でパケットを送信する。

【0176】ここで、移動計算機がホームネット外に移動した場合、後のパケット転送でゲートウェイに必要な制御を行ってもらうために、当該移動計算機、ホームエージェントあるいはホームネットのゲートウェイなどにより、移動計算機のホームネットでのアドレスと、獲得

したケア・オブ・アドレスの組を所定のデータベースに登録するようにする。このデータベースは、通信システム内のいずれかの場所に設置したサーバ装置に管理させ、あるいは各ゲートウェイに分散して管理させるなどし、各ゲートウェイから検索可能とする。

【0177】以下では、様々な位置関係にある計算機間でパケット通信が行われる場合の各ブロードの動作や使用されるパケット形式等について説明する。

【0178】まず、計算機やゲートウェイがどのようなパケット形式でパケットを送受信するかについての基本的なプロトコルについて説明する。

【0179】この場合は、固定ノードとは、移動計算機でない固定計算機、ホームネット内に位置する移動計算機、ホームエージェントを含む。

【0180】また、各ネットワークは、ゲートウェイに保護されているものとする。

【0181】次のP0-1～P0-3は、パケット転送にゲートウェイが介在しない場合である。

【0182】(P0-1) 送信元ノードが位置するネットワークと同一のネットワーク内に位置する固定ノードに対しては、送信元ノードから直接、通常のIP形式パケットが転送される(図19の通信相手CH・移動計算機MN、図21の通信相手CH→ホームエージェントHA、図23の移動計算機MN→通信相手CH等参照)。

【0183】(P0-2) 外部ノードである固定計算機同士は、直接、通常のIP形式で通信するものとする。

【0184】(P0-3) 外部ノードとして移動中の移動計算機同士は、経路最適化後は、直接、暗号化末端認証形式で通信する。

【0185】次のP2-1～P2-3は、通信する2台のノードが異なるネットワークに位置し、パケット転送に2台のゲートウェイが介在する場合である。

【0186】(P2-1) 第1の固定ノードaから第2の固定ノードbへのパケット転送が行われる場合(固定ノードa→GWa→インターネット→GWb→固定ノードb)

図11に示すように、固定ノードaは通常のIP形式でパケットを送信し、GWaは該パケットを暗号化／末端認証形式にして転送し、GWbは該パケットをIP形式にして転送する。末端認証は、GWa・GWb間で行われる。

【0187】(P2-2) 他部署ネットワークに移動中の移動計算機から固定ノードにパケットを転送する場合(移動計算機→GWa→インターネット→GWb→固定ノード)

(i) 移動計算機が自装置の送信したパケットを認証なしには外部へ通過させない他部署ネットワークに位置する場合

図12に示すように、移動計算機は暗号化／経路間認証形式でパケットを送信し、GWaは該パケットを暗号化

／経路間認証形式にて転送し、GWbは該パケットをIP形式にして転送する。末端認証は、移動計算機・GWb間で行われる。経路間認証は、移動計算機・Gwa間とGwa・GWb間で行われる。

【0188】(ii) 移動計算機が自装置の送信したパケットを認証なしに外部へ通過させる他部署ネットワークに位置する場合

図13に示すように、移動計算機は暗号化／末端認証形式でパケットを送信し、Gwaは該パケットを暗号化／経路間認証形式にして転送し、GWbは該パケットをIP形式にして転送する。末端認証は、移動計算機・GWb間で行われる。経路間認証は、Gwa・GWb間で行われる。

【0189】(P2-3) 固定ノードから他部署ネットワークに移動中の移動計算機にパケットを転送する場合（固定ノード→Gwa→インターネット→GWb→移動計算機）

ホームエージェントは、パケットを転送する場合には移動IP形式で、登録応答メッセージを送信する場合には通常のIP形式でパケットを送信する。また、経路最適化後において、移動計算機でない固定計算機またはホームに位置する移動計算機は、IP形式でパケットを送信する。

【0190】いずれの場合にも、Gwaはパケットを暗号化／経路間認証形式にて転送し、GWbは該パケットを暗号化／末端認証形式にして転送する。末端認証は、Gwa・移動計算機間で行われる。経路間認証は、Gwa・GWb間で行われる。

【0191】図14に、ホームエージェントがパケットを転送する場合について示す。

【0192】なお、ここでは、移動計算機が自装置の送信したパケットを認証なしに外部へ通過させない他部署ネットワークに位置する場合と、移動計算機が自装置の送信したパケットを認証なしに外部へ通過させる他部署ネットワークに位置する場合とで、同じの方法となる。

【0193】次のP1-1～P1-4は、パケット転送に1台のゲートウェイが介在する場合である。

【0194】(P1-1) 外部ノードとして移動中の移動計算機からGW保護域内に位置する固定ノードへの通信の場合（移動計算機→GW→固定ノード）

移動計算機は暗号化／末端認証形式でパケットを送信し、GWは該パケットを通常のIP形式にて転送する。末端認証は、移動計算機・GW間で行われる。

【0195】この場合を図15に示す。

【0196】(P1-2) GW保護域内に位置する固定ノードから外部ノードとして移動中の移動計算機への通信の場合（固定ノード→GW→移動計算機）

ホームエージェントは、パケットを転送する場合には移動IP形式で、登録応答メッセージを送信する場合には

通常のIP形式でパケットを送信する。また、経路最適化後において、移動計算機でない固定計算機またはホームに位置する移動計算機は、IP形式でパケットを送信する。

【0197】いずれの場合にも、GWはパケットを暗号化／末端認証形式にして転送する。末端認証は、GW・移動計算機間で行われる。

【0198】この場合を図15に示す。

【0199】(P1-3) 固定計算機である外部ノードがGW保護域内の固定ノードと通信する場合

この場合、暗号通信は行わないものとしているので、外部ノードとGWの間、GWと固定ノードの間では、通常のIP形式でパケット転送される。

【0200】なお、固定計算機である外部ノードが暗号化認証機能を備えているならば暗号通信可能とするケースをサポートする場合、上記のP1-1、P1-2と同様の動作になる。

【0201】(P1-4) 他部署ネットワークに移動中の移動計算機へ同一ネットワーク内の固定ノードからパケットを転送する場合で、かつ、経路最適化後の場合（固定ノード→GW→移動計算機）

固定ノードは通常のIP形式でパケットを送信すると、GWは該パケットを移動IP形式にして移動計算機に転送する。

【0202】次のPz-1～Pz-3は、セキュリティポリシーに応じて種々のケースが考えられる。

【0203】(Pz-1) 外部ノードとして移動中の移動計算機が固定計算機である外部ノードと通信しようとする場合

後述するように、ホームネットワークのブロキシーを介した通信とする。

【0204】従って、移動計算機とゲートウェイの間でのパケット通信には暗号化／末端認証形式が使用され、固定計算機とゲートウェイの間でのパケット通信には通常のIPが使用される。

【0205】(Pz-2) 他部署ネットワークに移動中の移動計算機が固定計算機である外部ノードと通信しようとする場合

暗号通信を行わないものとする。

【0206】(Pz-3) 上記のPz-2で、経路最適化する場合

移動計算機と固定計算機は、暗号通信を行わずに、ゲートウェイを介して直接通信するものとする。

【0207】なお、Pz-2とPz-3において、移動計算機から固定計算機宛のパケットのみ、ゲートウェイを通過させるために移動計算機・ゲートウェイ間で認証を行っても良い（例えば暗号化／末端認証形式を使用する）。

【0208】上記のプロトコルを送信元となる計算機についてまとめると、次のようになる。

【0209】・固定計算機は、常に通常のIP形式のバケットを送信する。

【0210】・ホームエージェントは、移動計算機へのバケット転送を行う場合、移動IP形式を使用する。ただし、登録応答メッセージは、IP形式での送信となる。

【0211】・移動計算機は、自装置の位置する場所を認識した結果により、以下のように動作が異なってくる。

【0212】(S1) 自装置がホームに位置する場合、通常のIP形式のバケットを送信する。

【0213】(S2) 自装置が現在位置するネットワーク内に宛先計算機が位置すると認識された場合、通常のIP形式のバケットを送信する。

(S3) 移動先のネットワークのゲートウェイが自装置の送信するバケットを認証した後に外部へ通過させる場合、宛先計算機がその移動先ネットワークの外部に位置するとき、暗号化/経路間認証形式のバケットを送信する。

(S4) 移動先のネットワークのゲートウェイが自装置の送信するバケットを認証なしに外部へ通過させる場合、宛先計算機がその移動先ネットワークの外部に位置するとき、暗号化/末端認証形式のバケットを送信する。

(S5) 自装置が現在外部ノードとして移動している場合、暗号化/末端認証形式のバケットを送信する。

【0214】(S6) ただし、S4とS5において、相手計算機が外部ノードである固定計算機の場合、上記のPz-2やPz-3の手順によっては、相手計算機が外部ノードである固定計算機であるか否かに応じて、バケット形式を選択する場合がある。すなわち、Pz-2とPz-3において、移動計算機・ゲートウェイ間で認証を行わない場合、通常のIP形式を使用する(例外処理となる)。一方、移動計算機・ゲートウェイ間で認証を行う場合、暗号化/末端認証形式を使用する。後者の場合、S4とS5において、相手計算機が外部ノードである固定計算機であるか否かにかかわらず、バケット形式は統一される。

【0215】移動計算機は、図3で説明した位置認識部により、自装置の現在位置が、ホームネット内部か、ホームネット外部か、外部ノードかを認識することができる。また、外部ノードでない場合、自装置を現在、暗号化認証処理対象とするゲートウェイを知ることができる。

【0216】また、移動計算機は、通信相手の現在の位置を認識する通信相手位置認識部を持つ。例えば、前述した各ゲートウェイについてそれが暗号化認証処理対象とする計算機の情報を登録したデータベースを検索することにより実現できる。

【0217】なお、通信相手が移動計算機でホームネッ

ト外に移動中の場合、移動計算機のホームネットでのアドレスをもとに検索等を行うので、移動計算機のホームネットのゲートウェイが認識される。

【0218】図16に、通信相手の位置を検出する処理の一例を示す。

【0219】通信相手のIPアドレスから対応するアドレスを保護域とするゲートウェイ(GW通信相手CH)を検索する(ステップS21)。検索にかからなければ通信相手はGW保護域外であると認識する。

【0220】通信相手がGW保護域内の場合(ただしそのゲートウェイが自装置を現在、暗号化処理対象とするゲートウェイと異なる場合)、後のデータ通信で必要となるので、通信相手のホームネットのゲートウェイの暗号化/認証用公開鍵を取得する(ステップS23)。例えば、自装置のホームネットワークのゲートウェイもしくは別途設置した管理サーバに問い合わせる。なお、該当する鍵を既に持っている場合にはこの手続きは不要である。

【0221】なお、上記の(S3)と(S4)について、移動先のネットワークのゲートウェイが自装置の送信するバケットを認証した後に外部へ通過させるか、認証なしに外部へ通過させるかは、前述した登録メッセージに関する手順を行った結果から知ることができる。すなわち、暗号化/末端認証形式で送信した登録メッセージに対して通過拒否された場合は(S3)に該当し、暗号化/末端認証形式で送信した登録メッセージが受諾され通過された場合は(S4)に該当する。

【0222】次に、各ゲートウェイは、種々の条件に応じて、ある形式のバケットを、そのまま、あるいは同じ形式で内容を変えてあるいは、あるいは異なる形式に変換して転送する。

【0223】各ゲートウェイは、入力バケットのヘッダ情報から送信元となる計算機や宛先となる計算機の情報を読取り、この情報をもとに所定のデータベース等を検索するなどして、必要な情報を得ることができる。

【0224】各ゲートウェイは、バケットの転送に係る計算機が、ホームネット外に移動中の移動計算機か否かを認識する移動計算機認識部と、バケットの転送に係る計算機について、これを暗号化処理対象とする計算機を認識するゲートウェイ認識部とを備える。また、前述したように、自装置が現在、暗号化認証処理対象とする計算機を認識する暗号化認証処理対象計算機認識部を持つ。

【0225】移動計算機認識部は、例えば、前述したホームネット外に移動中の移動計算機に関する登録を行ったデータベースを検索することにより実現できる。

【0226】ゲートウェイ認識部は、前述した移動計算機の通信相手位置認識部と同様で、各ゲートウェイについてそれが暗号化認証処理対象とする計算機の情報を登録したデータベースを検索することにより実現できる。

【0227】なお、通信相手がGW保護域内の場合（ただしそのゲートウェイが自装置を現在、暗号化処理対象とするゲートウェイと異なる場合）、後のデータ通信で必要となるので、通信相手のホームネットのゲートウェイの暗号化／認証用公開鍵を取得する。例えば、自装置のホームネットワークのゲートウェイもしくは別途設置した管理サーバに問い合わせる。なお、該当する鍵を既に持っている場合にはこの手続きは不要である。

【0228】。

【0229】また、ゲートウェイは、計算機等から経路最適化の要求を受けた場合あるいは自発的に、移動計算機認識部やゲートウェイ認識部による認識結果をもとにして、経路最適化が可能か否かを判定するとともに、経路最適化が可能で自装置が経路最適化に寄与するものと認識された場合、認識結果に応じた経路を最適化するための制御を行う経路最適化制御部を備えても良い。

【0230】経路最適化制御部では、最適化前でのパケットに対する処理内容を、最適化後でのパケットに対する処理内容に変更する。

【0231】ここで、ゲートウェイと計算機がパケット処理のために用いるホームネット外に移動中の移動計算機や固定計算機の位置情報（各計算機を保護するゲートウェイの情報）の管理についてさらに説明する。

【0232】各計算機の位置情報は、各々の計算機自身が発して他のノードに通知するように構成することが可能である。

【0233】この場合、位置情報の通知方式としては、例えば、以下の2つの方法が考えられる。

【0234】（1）データベースで管理する方法

各計算機が夫々現在の位置情報（自装置を暗号化処理対象とするゲートウェイのアドレス情報）を中央のデータベースに報告し、以降、その情報が必要なノードは、そのデータベースに問い合わせを行って処理を進める。データベースはシステム内の任意の位置に置いて構わないが、移動計算機がホームネット外に移動した際に情報が更新される点を考慮すると、例えば、移動計算機のホームネットワーク内の移動計算機位置情報管理装置内に置くのが便利である。

【0235】（2）データ転送に伴って、経路途中の構成要素に通知する方法

各計算機が最初のデータを転送する際に、そのデータパケットの一部分に自身の位置情報を入れ、これを経路途中のノードが取り出して、当該ノードの持つ位置情報キャッシュに格納する。この方法は、位置情報を一元管理できないが、データ転送に伴って位置情報を伝搬でき、別のアクセスが不要になるので効率の点では有利である。

【0236】さて、ゲートウェイは、前述の移動計算機認識部やゲートウェイ認識部による認識結果に応じて、計算機間での通信にどのようなプロトコルが適用される

のかを判断し、また入力パケットをどのように処理して転送するかを判断し、例えば以下に示すような所定の処理を行う。

【0237】（G1）パケット転送を行ういずれの計算機も固定ノードであり、かつ、いずれの計算機についてもゲートウェイの存在が確認された場合、ゲートウェイは、通常のIP形式が来たら、暗号／末端認証形式にカプセル化し、暗号／末端認証形式が来たら、通常のIP形式にデカプセル化する。末端認証はゲートウェイ間で行う。

【0238】（G2）少なくとも一方の計算機が、ホームネット外に移動中の移動計算機で、かつ、いずれの計算機も自装置を暗号化認証処理対象とするゲートウェイを持たない固定ノードではないことが認識された場合は、以下のようになる。

【0239】（i）通常のIP形式が来たら、暗号／末端認証形式にカプセル化し、暗号／末端認証形式が来たら、通常のIP形式にデカプセル化する（経路最適化に係るゲートウェイを除く）。末端認証はゲートウェイ間で行う。

【0240】ただし、次の2つは例外処理となる（例えば、ヘッダ情報から制御メッセージであることを認識して処理を行う）。

【0241】ホームエージェント発、ホームネット外に移動中で自装置を暗号化認証処理対象とするゲートウェイを持たない移動計算機宛のIP形式のパケット（例えば、登録確認メッセージ）については、末端認証はゲートウェイ・移動計算機間で行う。

【0242】また、ホームエージェント発、ホームネット外に移動中で自装置を暗号化認証処理対象とするゲートウェイを持つ移動計算機宛のIP形式のパケット（例えば、登録確認メッセージ）については、暗号／経路間認証形式にカプセル化して転送する。末端認証はゲートウェイ・移動計算機間で行い、経路間認証はゲートウェイ間で行う。

【0243】（ii）ホームネット外に移動中の移動計算機（自装置が暗号化認証処理対象とするもの）発の暗号化／末端認証形式パケットまたは暗号化／経路間認証形式パケットが来たら、暗号化／経路間認証形式パケットを次段に転送する。

【0244】（iii）次段が外部から移動中の移動計算機（自装置が暗号化認証処理対象とするもの）である、暗号化／経路間認証形式パケットが来たら、暗号化／末端認証形式パケットを転送する。

（iv）次段が固定ノードである（自装置を末端認証の受信側とする）暗号化／末端認証形式パケットまたは暗号化／経路間認証形式パケットが来たら、デカプセル化してIP形式のパケットを転送する。

【0245】（v）移動IP形式のパケットが来たら、宛先計算機がホームネット外に移動中の計算機であり、

10

20

30

40

50



かつこの計算機を暗号化認証処理対象とするゲートウェイが存在する場合、暗号化／経路間認証形式パケットにして転送し、宛先計算機がホームネット外に移動中の計算機であり、かつこの計算機を暗号化認証処理対象とするゲートウェイが存在しない場合、暗号化／末端認証形式パケットにして転送する。

〔0246〕(vi) 経路最適化に係るゲートウェイは、経路最適化の要求を契機とし、例外処理として各ケースに応じた処理を行う。

〔0247〕(G3) 一方の計算機が固定計算機、他方の計算機がホームネット外に移動中の計算機で、かついずれの計算機も自装置を暗号化認証処理対象とするゲートウェイを持たない場合、固定計算機を送信元または宛先とする通常のIP形式のパケットが来たら、通常のIP形式のパケットを転送し、移動計算機を宛先とするIP形式または移動IP形式のパケットが来たら、暗号化／末端認証形式のパケットにして転送し、暗号化／末端認証形式のパケットが来たら、通常のIP形式のパケットにして転送する。

〔0248〕(G4) 一方の計算機が固定計算機で、この計算機を暗号化認証処理対象とするゲートウェイが存在せず、かつ、他方の計算機を暗号化認証処理対象とするゲートウェイが存在する場合、入力したパケットと同一形式で、パケットを転送する。

〔0249〕ただし、他方の移動計算機の移動先のゲートウェイが、一方の計算機が固定計算機でかつこの計算機を暗号化認証処理対象とするゲートウェイが存在しないときでも、認証なしにはパケットを通過させないようにするセキュリティ・ポリシーを採用する場合、移動計算機は、当該ゲートウェイとの間での認証コードを付加してパケットを送信し（例えば、暗号化／末端認証形式を用いる）、当該ゲートウェイは、認証チェックに成功したならば、IP形式のパケットを転送する。その他では、入力したパケットと同一形式で、パケットを転送する。

〔0250〕以下では、図1のネットワーク1aの内部にホームポジションを持つ移動計算機（移動計算機MN）2と固定ホストである通信相手計算機（通信相手CH）3とのパケット通信を例にとってより具体的に説明する。

〔0251〕まず、図1に示す通信システムにおいて、移動計算機2と固定ホストである通信相手3の存在する場所の組合せおよびその際の通信処理内容は、図17のように〔ケース1〕～〔ケース4〕の4つのケースに大分類される。

〔0252〕〔ケース1〕移動計算機MNがGW保護域内、通信相手計算機通信相手CHがGW保護域内であるケース

〔ケース2〕移動計算機MNがGW保護域外、通信相手計算機通信相手CHがGW保護域内であるケース

〔ケース3〕移動計算機MNがGW保護域内、通信相手計算機通信相手CHがGW保護域外であるケース

〔ケース4〕移動計算機MNがGW保護域外、通信相手計算機通信相手CHがGW保護域外であるケース

さらに、上記の〔ケース1〕〔ケース2〕のゲートウェイGWを介した通信のケースを細分類すると、図18に示すように、（ケース1）～（ケース7）の7つのケースに分類される（〔ケース1〕が（ケース1）～（ケース5）に細分類され、〔ケース2〕が（ケース6）と（ケース7）に細分類される）。

〔0253〕（ケース1）移動計算機MNはホームネット内、通信相手計算機通信相手CHも移動計算機MNのホームネット内に位置するケース

（ケース2）移動計算機MNはホームネット内、通信相手計算機通信相手CHは他部署ネット内に位置するケース

（ケース3）移動計算機MNは他部署ネット内、通信相手計算機通信相手CHは移動計算機MNのホームネット内に位置するケース

（ケース4）移動計算機MNは他部署ネット内、通信相手計算機通信相手CHも移動計算機MNと同じネット内に位置するケース

（ケース5）移動計算機MNはいずれかの他部署ネット内、通信相手計算機通信相手CHは移動計算機MNと異なる他部署ネット内に位置するケース

（ケース6）移動計算機MNは外部ノード、通信相手計算機通信相手CHは移動計算機MNのホームネット内に位置するケース

（ケース7）移動計算機MNは外部ノード、通信相手計算機通信相手CHは他部署ネット内に位置するケース  
各々のケースについて、各ノードの処理、各ゲートウェイでのIPセキュリティ処理が異なることがある。前述したように、通信相手3の位置によっては、暗号通信を使用できない場合もある。例えば、通信相手3がパケット暗号化認証処理を行うパケット処理装置のないネットワークにいる場合である。これは上の〔ケース3〕〔ケース4〕の場合に相当する。このような場合は、移動計算機は、移動IPプロトコルのみを使用し、パケットの暗号化を行わないことになる。または、通常のIP通信のみで、移動処理も行わないようにしても良い。

〔0254〕また、移動IPでは、ホームエージェント経由の移動計算機宛のパケット経路を、各ネットワーク構成要素が正しい位置情報をキャッシュして保持している場合に最適化することを規定している。この経路最適化も、パケット暗号化を併用する場合、移動計算機と通信相手の現在位置を認識して、適用可能性を判定することが必要になる。

〔0255〕以上のように、移動IP、IPセキュリティの併用する際には移動計算機、通信相手の位置情報を検出し、上記（ケース1）～（ケース7）と上記〔ケー



ス3〕〔ケース4〕のように通信相手がGW保護域外にいるケースを認識するなどして、各ネットワーク構成要素の処理を制御することが非常に重要になる。

〔0256〕以下、上記の(ケース1)～(ケース7)、〔ケース3〕、〔ケース4〕の各ケースごとに説明を行う。

〔0257〕(ケース1)移動計算機MNと通信相手CHがともにホームネット1aに位置する場合

この場合、移動計算機は固定ノードであるので、前述のP0-1に該当する。

〔0258〕また、移動計算機が送信するパケットの形式は、前述のS1とS2に該当する(いずれの判断によっても良い)。

〔0259〕図19に示すように、移動計算機MNと通信相手CHは通常のIPパケット形式で直接通信する。

〔0260〕なお、ゲートウェイは介在しないので処理を行わない。

〔0261〕(ケース2)移動計算機MNはホームネット1a、通信相手CHが他部署ネット1bの場合

この場合、移動計算機は固定ノードであるので、前述のP2-1に該当する。

〔0262〕また、移動計算機が送信するパケットの形式は、前述のS1に該当する。

〔0263〕図20に示すように、移動計算機MNは通常のIPパケット形式を送出する。

〔0264〕ゲートウェイでは、IPパケット形式が来たら、暗号/末端認証形式にカプセル化し、暗号/末端認証形式が来たら、IPパケット形式にデカプセル化する。

〔0265〕(ケース3)移動計算機MNは他部署、通信相手CHがホームネットの場合

この場合、移動計算機MN→通信相手CHがP2-2に該当し、通信相手CH→ホームエージェントHAがP0-1に該当し、ホームエージェントHA→移動計算機MNがP2-3に該当する。

〔0266〕また、移動計算機が送信するパケットの形式は、前述のS3またはS4のいずれかに該当する。

〔0267〕P2-3(i)の場合を、図21に示す。

〔0268〕図22に示すように、移動計算機MNは暗号化/経路間認証形式のパケットを送信する。

〔0269〕各ゲートウェイでは、以下のパケット処理を行う。

〔0270〕・移動計算機MN発の暗号化/経路間認証形式パケットが来たら、暗号化/経路間認証形式パケットを次段に転送する。

・次段が移動計算機MNの、暗号化/経路間認証形式パケットが来たら、暗号化/末端認証形式パケットを転送する。

・それ以外の暗号化/経路間認証形式パケットが来たら、デカプセル化してIP形式パケットを転送する。

・移動IP形式のパケットが来たら、暗号化/経路間認証形式パケットにして転送する。

〔0271〕(ケース4)移動計算機MNと通信相手CHは同一の他部署の場合

この場合、移動計算機MN→通信相手CHがP0-1に該当し、通信相手CH→ホームエージェントHAがP2-1に該当し、ホームエージェントHA→移動計算機MNがP2-3に該当する。

〔0272〕また、移動計算機が送信するパケットの形式は、前述のS2に該当する。

〔0273〕P2-3(1)の場合を、図23に示す。

〔0274〕図24に示すように、移動計算機MNは通常のIPパケット形式を送出する。

〔0275〕ゲートウェイでは、以下のパケット処理を行う。

〔0276〕・IPパケット形式が来たら、暗号/末端認証形式パケットを転送する。

・暗号/末端認証形式パケットが来たら、デカプセル化してIP形式パケットを転送する。

・移動IP形式パケットが来たら、暗号化/経路間認証形式パケットを転送する。

・次段が移動計算機MNの、暗号化/経路間認証形式パケットが来たら、暗号/末端認証形式パケットを転送する。

〔0277〕ここで、経路最適化が要求された場合は、図25に示すように、該当するゲートウェイは、通信相手CHからのIP形式パケットを受信したら、移動IP形式パケットを移動計算機MNに転送するように制御する(P1-4に該当)。

〔0278〕(ケース5)移動計算機MNは他部署、通信相手CHは別の他部署の場合

この場合、移動計算機MN→通信相手CHがP2-2に該当し、通信相手CH→ホームエージェントHAがP2-1に該当し、ホームエージェントHA→移動計算機MNがP2-3に該当する。

〔0279〕また、移動計算機が送信するパケットの形式は、前述のS3またはS4に該当する。

〔0280〕P2-3(i)の場合を、図26に示す。

〔0281〕図27に示すように、移動計算機MNは暗号化/経路間認証形式のパケット形式を送出する。

〔0282〕ゲートウェイでは、以下のパケット処理を行う。

〔0283〕・IPパケットが来たら、暗号化/末端認証形式パケットを転送する。

・暗号化/末端認証形式パケットが来たら、デカプセル化してIPパケットを転送する。

・移動IPパケット形式が来たら、暗号化/経路間認証形式パケットを転送する。

・移動計算機MN発の、暗号化/経路間認証形式パケットが来たら、暗号化/経路間認証形式パケットを転送す

る。

・次段が移動計算機MNの、暗号化／経路間認証形式パケットが来たら、暗号化／末端認証形式パケットを転送する。

・それ以外の暗号化／経路間認証形式パケットが来たら、デカプセル化してIP形式パケットを転送する。

【0284】ここで、経路最適化が要求された場合を、図28に示す。

【0285】この場合、通信相手CH→移動計算機MNがP2-3に該当する。

【0286】この場合、各ゲートウェイが以下のパケット処理を行うように制御する。

【0287】・移動計算機MN発の、暗号化／経路間認証形式パケットが来たら、暗号化／経路間認証形式パケットを転送する。

・次段が移動計算機MNの、暗号化／経路間認証形式パケットが来たら、暗号化／認証形式パケットを転送する。

・それ以外の暗号化／経路間認証形式パケットが来たら、デカプセル化してIP形式パケットを転送する。

【0288】・通信相手CHからのIP形式パケットが来たら、暗号化／経路間認証形式パケットを転送する。

【0289】（ケース6）移動計算機MNは外部、通信相手CHはホームの場合

この場合、移動計算機MN→通信相手CHがP1-1に該当し、通信相手CH→ホームエージェントHAがP0-1に該当し、ホームエージェントHA→移動計算機MNがP1-2に該当する。

【0290】また、移動計算機が送信するパケットの形式は、前述のS5に該当する。

【0291】この場合を、図29に示す。

【0292】図30に示すように、移動計算機MNは暗号化／末端認証形式のパケットを送出する。

【0293】ゲートウェイでは、以下のパケット処理を行う。

【0294】・暗号化／末端認証形式パケットが来たら、デカプセルしてIPパケットを転送する。

・移動IP形式が来たら、暗号化／経路間認証形式パケットを転送する。

【0295】（ケース7）移動計算機MNは外部、通信相手CHは他部署の場合

この場合、移動計算機MN→通信相手CHがP1-1に該当し、通信相手CH→ホームエージェントHAがP2-1に該当し、ホームエージェントHA→移動計算機MNがP1-2に該当する。

【0296】また、移動計算機が送信するパケットの形式は、前述のS5に該当する。

【0297】この場合を、図31に示す。

【0298】図32に示すように、移動計算機MNは暗号化／末端認証形式のパケット形式を送出する。

【0299】ゲートウェイでは、以下のパケット処理を行う。

【0300】・IPパケットが来たら、暗号化／末端認証形式パケットを転送する。

・暗号化／末端認証形式パケットが来たら、デカプセルしてIPパケットを転送する。

・移動IP形式が来たら、暗号化／末端認証形式パケットを転送する。

【0301】ここで、経路最適化が要求された場合を、図33に示す。

【0302】この場合、通信相手CH→移動計算機MNがP1-2に該当する。

【0303】この場合、各ゲートウェイが以下のパケット処理を行うように制御する。

【0304】・暗号化／末端認証形式パケットが来たら、デカプセルしIPパケットを転送する。

・通信相手CHからのIP形式パケットを受信したら、暗号化／末端認証形式パケットをMHに転送する。

【0305】（ケース8）通信相手CHが保護域外、移動計算機MNがホームの場合（上記【3】の場合）  
図34に示すように、通常のIP通信のみを行う。

【0306】したがって、ゲートウェイでは暗号化認証処理は行わない。

【0307】（ケース9）通信相手CHが保護域外、移動計算機MNが外部の場合（上記【4】の場合）

図35に示すように、通常の移動IP通信のみを行い、ゲートウェイでは暗号化は行わないものとする。

【0308】または、図36に示すように、移動計算機MNは移動先で得たケア・オブ・アドレスを使った通常のIP通信を行い、移動IPと暗号化は行わないようにしても良い。

【0309】なお、他部署ネットワーク1cのセキュリティ・ポリシーに応じて、図35や図36において、移動計算機2発のパケットをゲートウェイ4cから外部に転送する場合に、移動計算機2とゲートウェイ4cとの間でのみ、認証を行うようにしても良い。

【0310】（ケース10）通信相手CHが保護域外、移動計算機MNが外部の場合（上記【4】の場合）  
この場合を、図37に示す。

【0311】以下のような処理を行うものとする。

【0312】・移動計算機MNは一旦ホームドメインに向かって暗号化／末端認証形式でパケットを送信する（送信元アドレスはプライベート・アドレスとする）。

・ホームドメインのプロキシ12でグローバル・アドレスに変換され、IPパケットが外部に行く。

・帰りはプロキシ12とホームエージェントHAを経由し、ゲートウェイ4aから暗号化／末端認証形式で移動計算機MNに届く。

【0313】以上では、図1のネットワーク1aの内部にホームポジションを持つ移動計算機（移動計算機M

N) 2と固定ホストである通信相手計算機(通信相手CH) 3とのパケット通信を例にとってより具体的に説明した。

【0314】以下では、ホームネット外に移動中の計算機間でのパケット通信についてより具体的に説明する。

【0315】ホームネット外に移動中の計算機間でのパケット通信は、次の各ケースに分類される。

【0316】<1>2つの計算機ともGW保護域内の場合

・異なるホームネットで、同じ他部署ネット(どちらのホームネットでもない)に位置するケース

・異なるホームネットで、異なる他部署ネット(どちらのホームネットでもない)に位置するケース

・異なるホームネットで、異なる他部署ネット(一方はいずれかのホームネット)に位置するケース

・異なるホームネットで、互いに通信相手のホームネットに位置するケース

・同じホームネットで、同じ他部署ネットに位置するケース

・同じホームネットで、異なる他部署ネットに位置するケース

・なお、上記の夫々のケースの夫々の他部署ネットについて、移動計算機の移動先ネットワークのゲートウェイが、自装置の装置するパケットを認証なしに外部へ通過させる場合と、そうでない場合がある。

【0317】<2>1つの計算機のみがGW保護域内(他部署ネットと外部ノード)の場合

・ホームネットが異なる場合

・ホームネットが同じ場合

・なお、上記の夫々のケースの夫々の他部署ネットについて、移動計算機の移動先ネットワークのゲートウェイが、自装置の装置するパケットを認証なしに外部へ通過させる場合と、そうでない場合がある。

【0318】<3>2つの計算機ともGW保護域外(外部ノード同士)の場合

・ホームネットが異なる場合

・ホームネットが同じ場合

以上の各ケースに分類されるが、前述したように、ホームネット外に移動中の計算機間でのパケット通信は、経路最適化前は、常に通信相手CHのホームエージェントHAを介して行われるので、各計算機やゲートウェイの動作は、上記した移動計算機と固定計算機との通信の場合に帰結される。

【0319】以下では、上記の各ケースのうちのいくつかについてのみ(移動計算機の移動先ネットワークのゲートウェイが、自装置の装置するパケットを認証チェックした後に外部へ通過させる場合について)説明し、その他のケースについては容易に類推可能であるため説明を省略する。

【0320】なお、移動計算機は、通信相手のホームエ

ージェントから発信される広告メッセージを受信した場合は、通信相手のホームネットに位置すると認識するものとする。

【0321】(C1)移動計算機MNは他部署、通信相手CHは別の他部署でいずれも通信相手CHのホームエージェントHAとは異なる場所の場合

この場合を、図38に示す。

【0322】図39に示すように、各移動計算機は暗号化/経路間認証形式のパケット形式を送出する。

【0323】例えば、計算機2-1からのパケットは通信相手2-2が移動しているため、通信相手2-2のホームネットワーク1dのゲートウェイ4dに転送され、ここで一旦復号され、通信相手2-2のホームエージェント5dに送られる。このホームエージェント5dで移動IP形式のカプセル化が行われ、通信相手2-2の現在の位置に転送される。

【0324】すなわち、この場合の移動計算機2-1→通信相手2-2のホームエージェント4dの転送経路は、例えば、(ケース5)で示した移動計算機MN→通信相手CHの転送経路における処理と同様になり、通信相手2-2のホームエージェント4d→通信相手2-2の転送経路は、(ケース5)で示したホームエージェントHA→移動計算機MNの転送経路における処理と同様になる。

【0325】言い換えると、前者は先に説明したP2-2のケースに該当し、後者はP2-3のケースに該当する。

【0326】したがって、ゲートウェイでは、以下のパケット処理を行うことになる。

【0327】・移動IPパケット形式が来たら、暗号化/経路間認証形式パケットを転送する。

・移動計算機MN発の、暗号化/経路間認証形式パケットが来たら、暗号化/経路間認証形式パケットを転送する。

・次段が移動計算機MNの、暗号化/経路間認証形式パケットが来たら、暗号化/認証形式パケットを転送する。

・それ以外の暗号化/経路間認証形式パケットが来たら、デカプセル化してIP形式パケットを転送する。

【0328】(C2)移動計算機MNは他部署で通信相手CHのホームエージェントHAが設置されたネット、通信相手CHは別の他部署(どちらのホームエージェントHAもないネット)の場合

この場合を、図40に示す。

【0329】計算機2-1を送信元とした場合は、図21のCHケース3で通信相手3を送信元とする場合と同様になる。

【0330】計算機2-2を送信元とした場合は、上記のC1のケースと同様になる。

【0331】ゲートウェイでは、以下のパケット処理を

行うことになる。

【0332】・移動IPバケット形式が来たら、暗号化／経路間認証形式バケットを転送する。

・移動計算機MN発の、暗号化／経路間認証形式バケットが来たら、暗号化／経路間認証形式バケットを転送する。

・次段が移動計算機MNの、暗号化／経路間認証形式バケットが来たら、暗号化／認証形式バケットを転送する。

・それ以外の暗号化／経路間認証形式バケットが来たら、デカプセル化してIP形式バケットを転送する。

【0333】したがって、ゲートウェイの処理は、上記のC1のケースと同様になる。

【0334】なお、上記の<1>のように2つの計算機ともGW保護域内の場合、いずれのケースも、ゲートウェイはケース5の6種類の動作のうちの一部を実行することになる。

【0335】次に、図41に示すように、上記の<2>の1つの計算機のみがGW保護域内（他部署ネットと外部ノード）のときに、2つの計算機が同じホームネットを持つ場合、先に説明したG2のケースにあるように、ゲートウェイは、ホームエージェント発、ホームネット外に移動中の計算機宛のバケットについて、宛先計算機に応じた処理を行う必要があるが、それ以外は、ケース5とケース6の動作のうちの一部を実行することになる。

【0336】次に、上記の<3>のように、2つの計算機ともGW保護域外（外部ノード同士）の場合、ゲートウェイは、ケース6の動作を実行することになる。

【0337】さて、従来、移動IP方式では、各ネットワークノードは一意なIPアドレスが付与され、自由に制御バケットをやりとりできるという假定でのみ、経路制御や移動計算機位置の登録などの規定を行っていたが、本実施形態によれば、実際の運用に再して、移動計算機がどのような組織に属するネットワークに移動したか、というネットワーク運用ポリシーに関する動作規定を考慮することができる。

【0338】また、IPセキュリティにもとづく暗号化装置を介して暗号化、認証通信を行う場合、各移動計算機、およびその通信相手の位置に応じて各ネットワーク構成要素の動作が大きく変化する。特に暗号化認証処理をとまって、移動IPの経路最適化を行うためにも、この位置情報認識を有効に利用できる。

【0339】また、移動IPの規定は、ネットワーク運用ポリシーを考慮していないため、例えば、外部組織のネットワークに移動して移動IPの登録メッセージをホームネットワーク宛に送信する場合、外部ネットワークのゲートウェイが外向きバケットをすべて許すのであれば、移動IPの規定がそのまま使用できるが、一般にこれはセキュリティの観点から望ましくない。したがっ

て、移動計算機は、自身が外部組織のネットワークにいる、ということ認識し、ゲートウェイに対して自分の身分証明を行う処理を行ってから外部アクセスを行うことが必要になり、本発明によれば、移動計算機が自身の現在位置を認識して現在接続しているネットワークから外へのアクセスを行う場合に必要な処理を正しく実行できる。

【0340】以上のように、本実施形態により、移動IPによる移動計算機の制御とIPセキュリティによるバケット暗号化処理をあわせて適用した場合に、実際のシステムで運用する場合の各ネットワークの管理ポリシーを反映し、かつ効率の良いシステム制御を実現できる。

【0341】なお、本実施形態では、固定計算機である外部ノードについては暗号通信をサポートしないものとして説明したが、固定計算機である外部ノードが暗号化認証機能を備えているならば暗号通信をサポートするようにしても良い。この場合、固定計算機である外部ノードのうち暗号化認証機能を備えているものを登録したデータベースをネットワーク中に設け、このデータベースを検索して固定計算機である外部ノードが暗号化認証機能を備えているならば、前述したP1-1（外部ノードとして移動中の移動計算機からGW保護域内に位置する固定ノードへの通信の場合）、P1-2（GW保護域内に位置する固定ノードから外部ノードとして移動中の移動計算機への通信の場合）と同様の処理を行うようにしても良い。

【0342】また、上記した各例では、移動先ネットワークにおいてそのゲートウェイから一旦バケットの通過を拒否された場合、所定の手順の後、認証データをバケットに付加して送信するものであったが、その代わりに、ゲートウェイにて認証に成功した移動計算機を管理対象として管理テーブルに登録し、以降はその移動計算機については認証を省くようにしても良い（この場合、登録後は、移動計算機は認証データをバケットに付加せずに送信することができる）。

【0343】また、本実施形態では、バケット転送に介在するゲートウェイGWは最大で2台であってが、例えば計算機を処理対象とするGWaとGWbとの間に、バケット転送に介在する他のGWeが介在する場合には、GWeは暗号化／経路間認証形式以外のバケットを受信した場合、そのまま通過させるようにしても良い。また、暗号化／経路間認証形式のバケットを転送する場合、GWaとGWe、GWeとGWbとの間で、それぞれ、経路間認証を行うようにしても良い。

【0344】以上の各機能、例えば移動計算機に搭載するバケット暗号化認証部などは、ハードウェアとしてもソフトウェアとして実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。

【0345】なお、本実施形態では、ポップアップモードによる通信システムについて説明したが、本発明は、フォーリンエージェントの存在を仮定した通信システムにも適用可能である。

【0346】また、本発明は、現在種々提案されている移動通信プロトコル、暗号化通信プロトコル、暗号鍵交換プロトコルに対しても適用可能である。

【0347】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0348】

【発明の効果】本発明に係る移動計算機装置によれば、ネットワーク運用ポリシーを考慮し自装置の現在位置に応じた適正なパケット転送を行うことができる。

【0349】また、本発明に係るパケット処理装置によれば、ネットワーク運用ポリシーを考慮しパケット通信する計算機の現在位置に応じた適正なパケット転送、暗号化認証処理、経路最適化などの通信制御を行うことができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るシステムの基本構成の一例を示す図

【図2】同実施形態で使用するパケット形式の一例を示す図

【図3】同実施形態に係る移動計算機による自装置の位置判定処理の流れを示すフローチャート

【図4】同実施形態に係る移動登録メッセージ送信手順を説明するための図

【図5】同実施形態に係る第1の登録メッセージのフォーマットの一例を示す図

【図6】同実施形態に係る通過拒否メッセージのフォーマットの一例を示す図

【図7】同実施形態に係る鍵要求メッセージのフォーマットの一例を示す図

【図8】同実施形態に係る第2の登録メッセージのフォーマットの一例を示す図

【図9】同実施形態でゲートウェイ間を転送される登録応答メッセージのフォーマットの一例を示す図

【図10】同実施形態で移動計算機が受信する登録応答メッセージのフォーマットの一例を示す図

【図11】同実施形態に係るノード間の通信の一例を示す図

【図12】同実施形態に係るノード間の通信の一例を示す図

【図13】同実施形態に係るノード間の通信の一例を示す図

【図14】同実施形態に係るノード間の通信の一例を示す図

【図15】同実施形態に係るノード間の通信の一例を示す図

【図16】同実施形態に係る移動計算機による通信相手の位置判定処理の流れを示すフローチャート

【図17】通信態様の分類を説明するための図

【図18】通信態様の分類を説明するための図

【図19】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図20】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

10 【図21】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図22】同実施形態で計算機の送信するパケット形式の一例を示す図

【図23】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図24】同実施形態で計算機の送信するパケット形式の一例を示す図

【図25】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

20 【図26】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図27】同実施形態で計算機の送信するパケット形式の一例を示す図

【図28】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図29】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図30】同実施形態で計算機の送信するパケット形式の一例を示す図

30 【図31】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図32】同実施形態で計算機の送信するパケット形式の一例を示す図

【図33】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図34】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図35】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

40 【図36】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図37】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図38】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図39】同実施形態で計算機の送信するパケット形式の一例を示す図

【図40】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

50 【図41】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図42】移動計算機を含む通信システムの基本構成を説明するための他の図

【図43】経路最適化を説明するための図

【符号の説明】

1, 1a, 1b, 1c, 1c…ネットワーク

2, 2-1, 2-2…移動計算機

\* 3…通信相手計算機

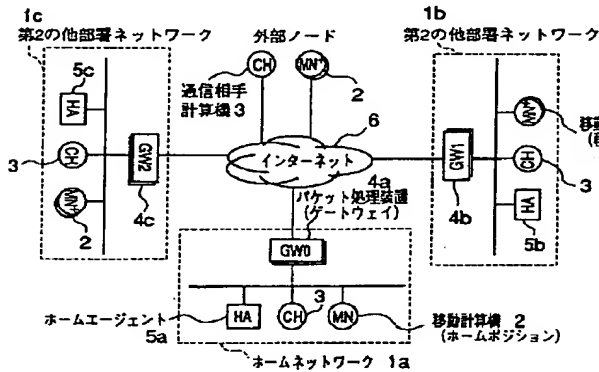
4, 4a, 4b, 4c, 4d…パケット処理装置（ゲートウェイ）

5, 5a, 5b, 5c, 5d…ホームエージェント

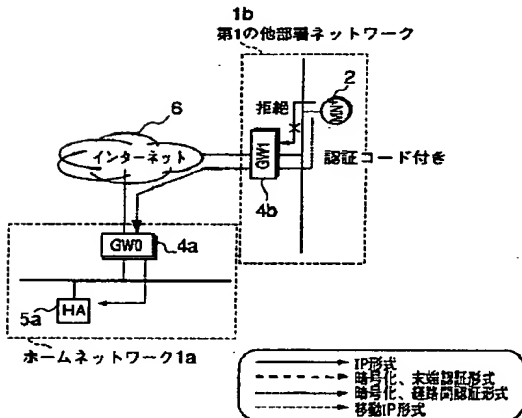
6…インターネット

\* 23…固定ノード

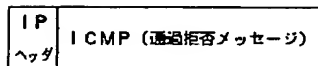
【図1】



【図4】

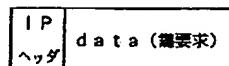


【図6】



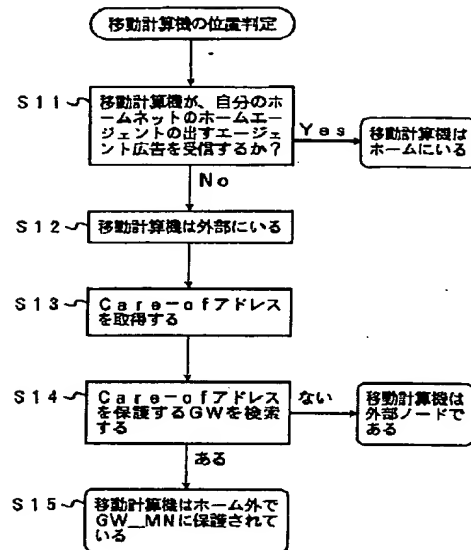
IPヘッダ (KEY)  
送信元=GW1のグローバル・アドレス  
宛 先=MNのケア・オブ・アドレス

【図7】

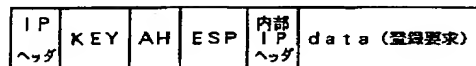


送信元=MNのケア・オブ・アドレス  
宛 先=GW1のグローバル・アドレス

【図3】



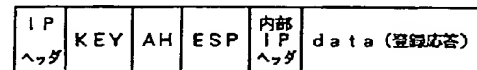
【図5】



IPヘッダ (KEY)  
送信元=MNのケア・オブ・アドレス  
宛 先=GW0のグローバル・アドレス

内部IPヘッダ (登録要求)  
送信元=MNのプライベート・アドレス  
宛 先=HAのプライベート・アドレス

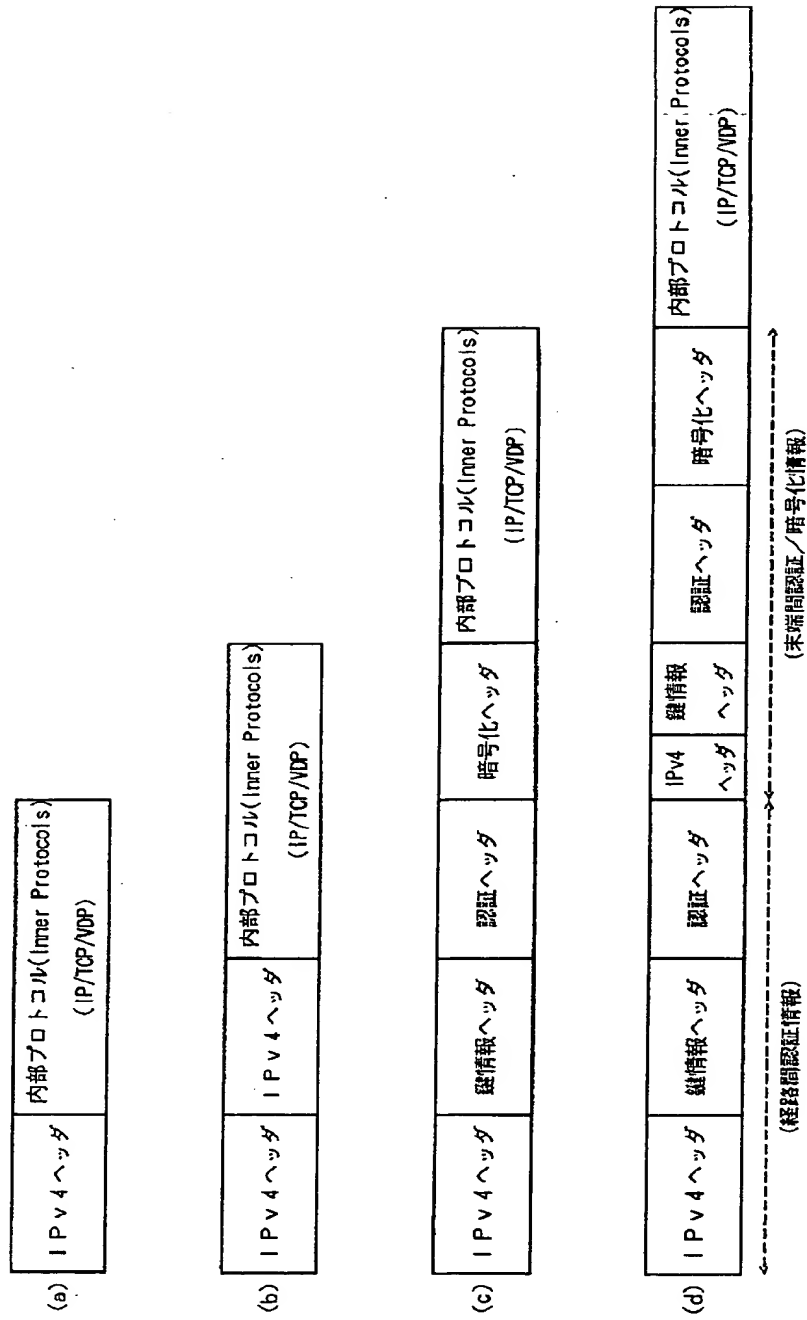
【図10】



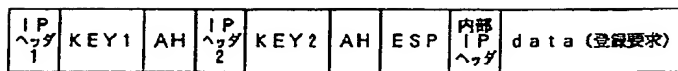
IPヘッダ  
送信元=GW0のグローバル・アドレス  
宛 先=MNのケア・オブ・アドレス

内部IPヘッダ (登録応答)  
送信元=HAのプライベート・アドレス  
宛 先=MNのプライベート・アドレス

【図2】



【図8】

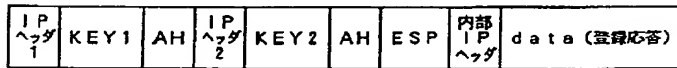


IPヘッダ1  
送信元=MNのケア・オブ・アドレス  
宛 先=GW1のグローバル・アドレス

IPヘッダ2  
送信元=MNのケア・オブ・アドレス  
宛 先=GW0のグローバル・アドレス

内部IPヘッダ (登録要求)  
送信元=MNのプライベート・アドレス  
宛 先=HAのプライベート・アドレス

【図9】

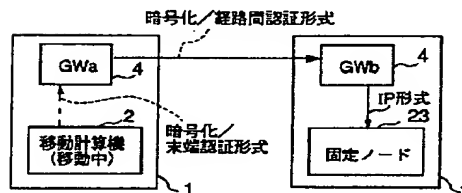


IPヘッダ1  
送信元=GW0のグローバル・アドレス  
宛 先=GW1のグローバル・アドレス

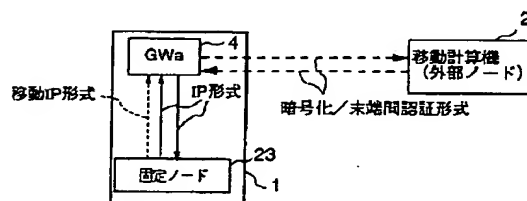
IPヘッダ2  
送信元=GW0のグローバル・アドレス  
宛 先=MNのケア・オブ・アドレス

内部IPヘッダ (登録応答)  
送信元=HAのプライベート・アドレス  
宛 先=MNのプライベート・アドレス

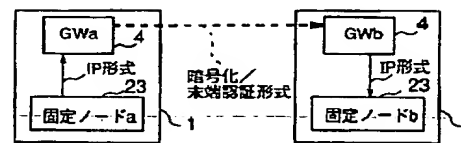
【図13】



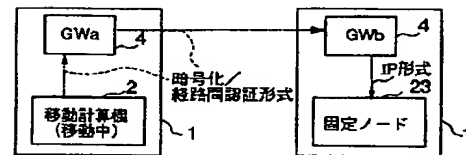
【図15】



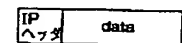
【図11】



【図12】

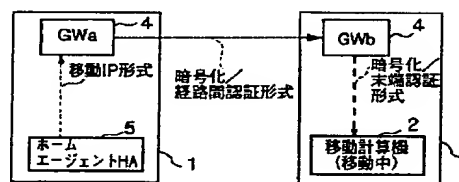


【図24】

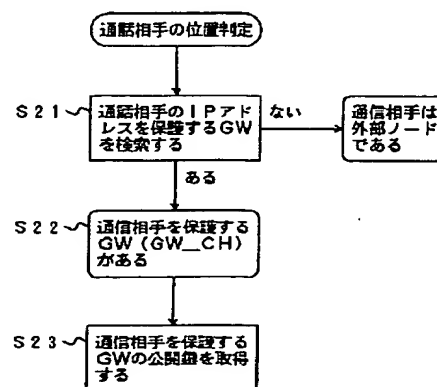


IPヘッダ(TCP/IP)  
送信元=MNのアドレス  
宛先=CHのアドレス

【図14】



【図16】





【図17】

通信相手計算機 CHの位置	GW保護域内	GW保護域外
移動計算機 MNの位置		
GW保護域内	[1] GWを介したIP CHアドレス: プライベート MNアドレス: プライベート	[3] 通常のIP CHアドレス: グローバル MNアドレス: プライベート →プロキシGWでグローバルに変換
GW保護域外	[2] GW*を介したIP CHアドレス: プライベート MNアドレス: プライベート	[4] 通常のIP CHアドレス: グローバル MNアドレス: プライベート MNはケアオブアドレスで普通 にIP通信 (もしくはホームのプロキシ を経由したIP. ホームまではVPN.)

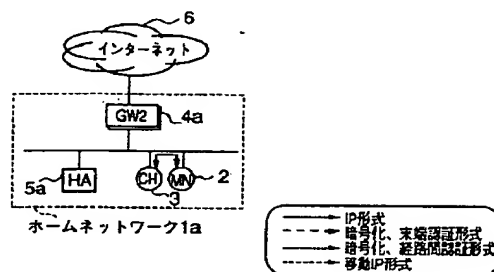
\*: MN付属のGW機能が動作するケース

【図18】

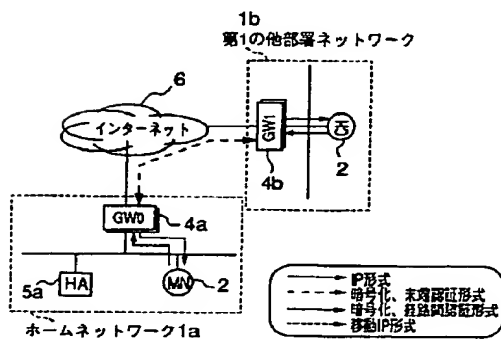
通信相手計算機 CHの位置	NMのホームネット	他 部 署 1
移動計算機 MNの位置		
ホームネット	(1)	(2)
他部署1	(3)*	(4)*
他部署2		(5)*
外 部	(6)*	(7)*

\*: MN付属のGW機能が動作するケース

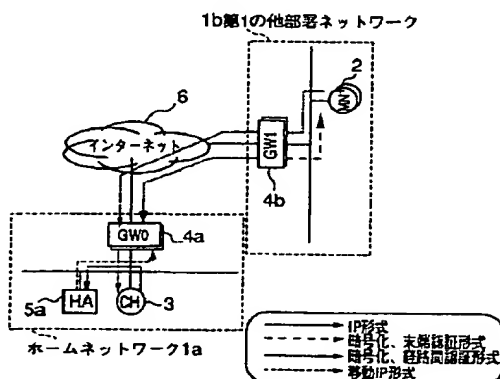
【図19】



【図20】



【図21】

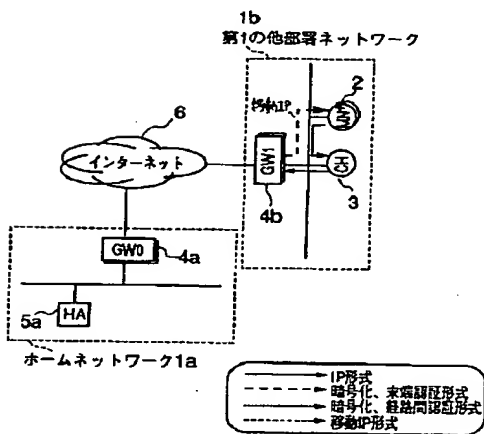


【図22】

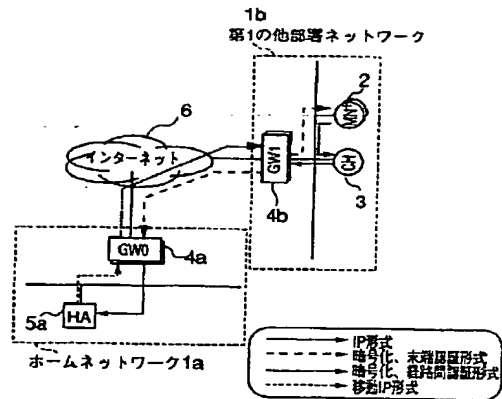
IPヘッダ1	KEY1	AH	IPヘッダ2	KEY2	AH	ESP	内部IPヘッダ	data
--------	------	----	--------	------	----	-----	---------	------

IPヘッダ1  
送信元=MNのケア・オブ・アドレス  
宛先=GW1(GW\_MN)のグローバル・アドレス  
IPヘッダ2  
送信元=MNのケア・オブ・アドレス  
宛先=GW2(GW\_CH)のグローバル・アドレス  
内部IPヘッダ (転送要求)  
送信元=MNのプライベート・アドレス  
宛先=CHのプライベート・アドレス

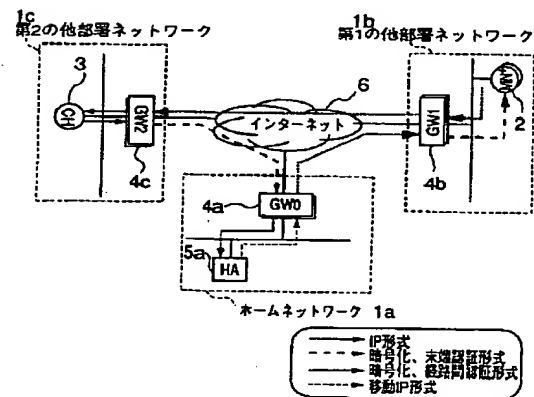
【図25】



【図23】



【図26】

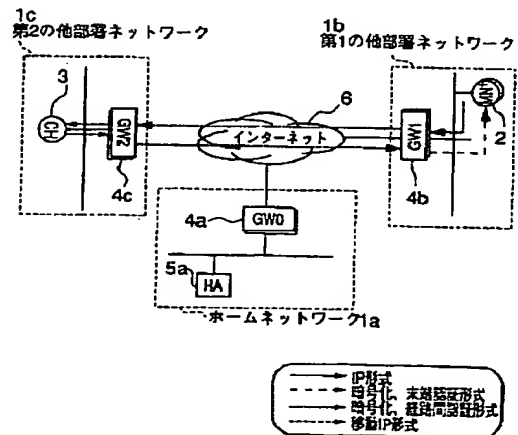


【図27】

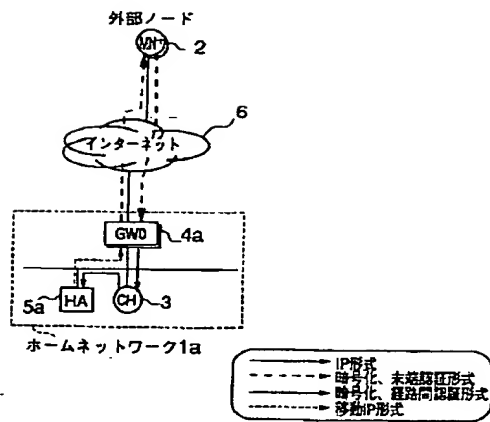
IPヘッダ1	KEY1	AH	IPヘッダ2	KEY2	AH	ESP	内部IPヘッダ	data
--------	------	----	--------	------	----	-----	---------	------

IPヘッダ1  
送信元=MNのケア・オブ・アドレス  
宛先=GW1(GW\_MN)のグローバル・アドレス  
IPヘッダ2  
送信元=MNのケア・オブ・アドレス  
宛先=GW2(GW\_CH)のグローバル・アドレス  
内部IPヘッダ (転送要求)  
送信元=MNのプライベート・アドレス  
宛先=CHのプライベート・アドレス

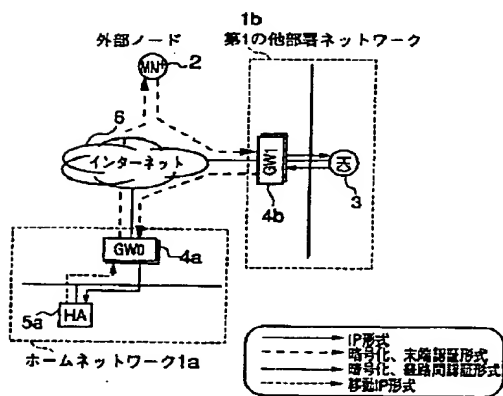
【図28】



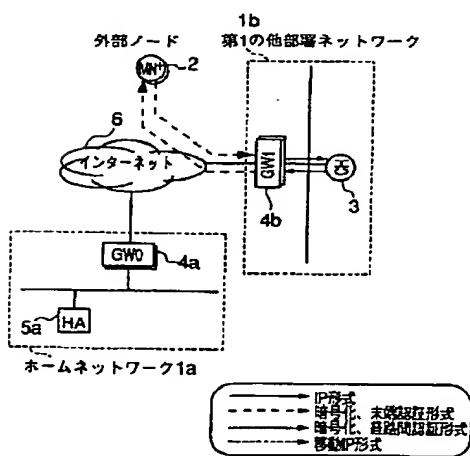
【図29】



【図31】



【図33】



【図30】

IP ヘッダ	KEY	AH	ESP	内部 IPヘッダ	data
-----------	-----	----	-----	-------------	------

IPヘッダ1

送信元=MNのケア・オブ・アドレス(グローバル・アドレス)

宛先=GW0(GW\_CH)のグローバル・アドレス

内部IPヘッダ

送信元=MNのプライベート・アドレス

宛先=CHのプライベート・アドレス

【図32】

IP	KEY	AH	ESP	内部IP	data
----	-----	----	-----	------	------

IPヘッダ1

送信元=MNのケア・オブ・アドレス(グローバル・アドレス)

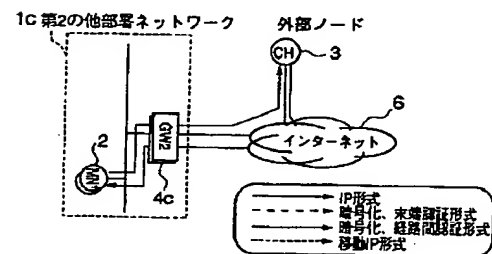
宛先=GW1(GW\_CH)のグローバル・アドレス

内部IPヘッダ

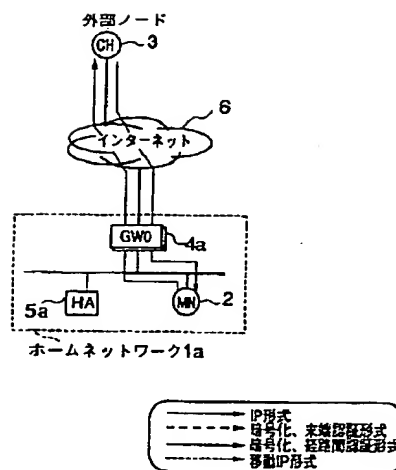
送信元=MNのプライベート・アドレス

宛先=CHのプライベート・アドレス

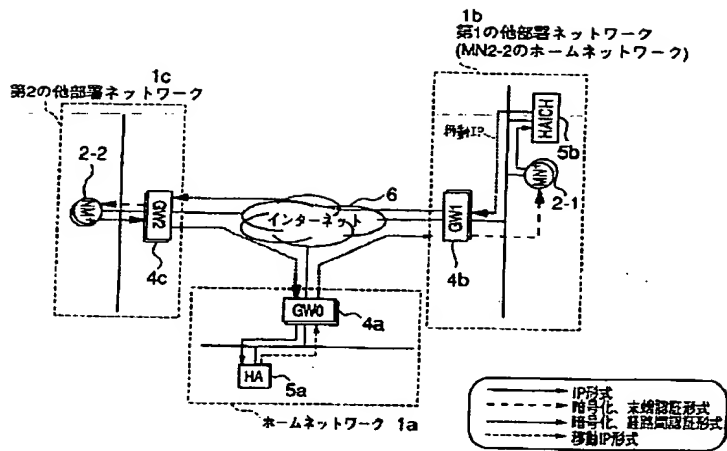
【図36】



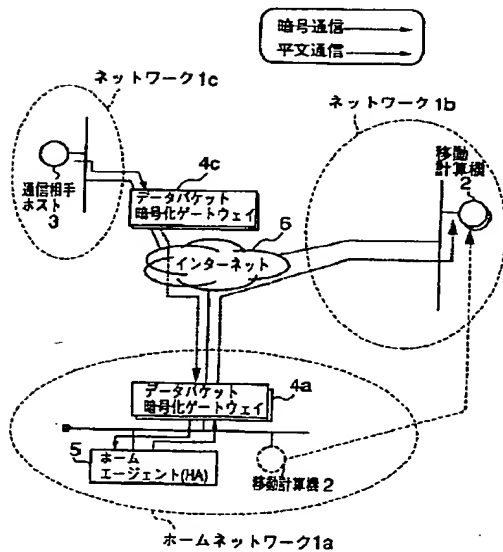
【図34】



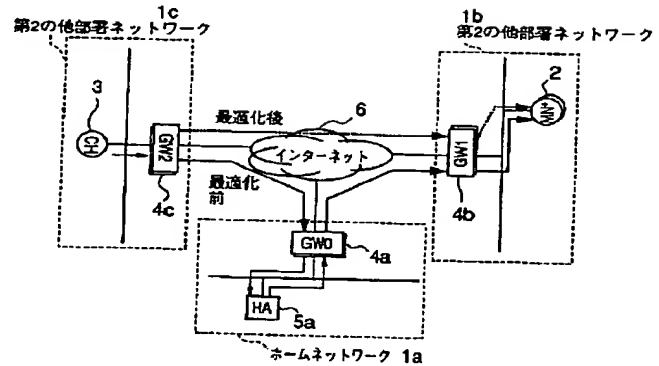
【図40】



【図42】



【図43】



フロントページの続き

(72)発明者 津田 悦幸  
 神奈川県川崎市幸区小向東芝町1番地 株  
 式会社東芝研究開発センター内

(72)発明者 新保 淳  
 神奈川県川崎市幸区小向東芝町1番地 株  
 式会社東芝研究開発センター内

(72)発明者 岡本 利夫  
 神奈川県川崎市幸区小向東芝町1番地 株  
 式会社東芝研究開発センター内